HP Insight Remote Support Advanced A.05.40 受管理系統手冊

HP 產品編號： 5900-0372
A.05.40 - 6.0 版 2010 年 1 月 18 日 出版



法律聲明

致謝

目錄

圖表清單

表格清單

關於本文件

目標讀者

本文件的使用對象爲安裝、設定及使用 Insight Remote Support Advanced A.05.40 的 HP 客戶與 HP 技術支援人員，他們可以在設定 CMS 之前和期間，使用本文件來驗證受管理系統是否已正確設定。

發佈記錄

早於 Insight Remote Support Advanced A.05.20 的版本已不再發行或支援。

製造組件編號	版本	變更摘要	版本編號	發佈日期
5900-0372	A.05.40	A.05.40 軟體版次的新版本	6.0	2010 年 1 月 18 日
5992-6223	A.05.30	A.05.30 軟體版次的新版本	5.0	2009 年 7 月 7 日
5993-6210	A.05.20	修訂版本，以包含 Virtual Libraries，以及適用於 Integrity Windows、Linux 及 HP-UX 受管理系統之 WBEM 設定的增強說明。	4.1	2009 年 3 月 6 日
5992-6302	A.05.20	Insight Remote Support Advanced A.05.20 的新版本	4.0	2009 年 1 月 27 日

產品概觀

Insight Remote Support Advanced 並非獨立的軟體應用程式。而是一組可一同運作以形成「遠端支援解決方案」的應用程式。Insight Remote Support Advanced 能夠提供回應式的主動式遠端支援，以提昇您資料中心內 HP 所支援之伺服器及相關儲存系統的可用性。

完整的 Insight Remote Support Advanced 解決方案仰賴數個 HP 元件，並會在客戶企業中的各種軟體應用程式之間，以及客戶企業與 HP 之間進行通訊，以提供這些支援服務。本文件說明在 CMS 上安裝或設定 Insight Remote Support Advanced 之前，爲您的受管理系統建立一個穩定環境所需的預先工作。軟體元件會根據其用途安裝於 CMS 或受管理系統上。Insight Remote Support Advanced 是一種含有許多變數的複雜解決方案，因此，請務必在繼續進行完整安裝 Insight Remote Support Advanced 之前，先仔細閱讀本文件。

縮寫指南

本指南附有正式詞彙表，本縮寫指南可供您快速參照本文件中常見的詞彙。

縮寫	正式詞彙	定義
ACC	進階設定收集器	ACC 規則安裝在 CMS 上。ACC 軟體安裝在 HP-UX 受管理系統 上。
CMS	中央管理伺服器	CMS 是管理網域中執行 HP Systems Insight Manager 軟體的系統。HP Systems Insight Manager 內所有的中央作業皆從此系統開始執行。
ELMC	Event Log Monitoring Collector	ELMC (先前稱做 WCCProxy) 提供事件日誌檔的錯誤狀況偵測，並將這些事件傳遞至 WEBES。

縮寫	正式詞彙	定義
EVA	企業虛擬陣列	EVA 是高效能、高容量與高可用性的虛擬 RAID 儲存解決方案，適合高階企業環境。
HP SIM	Hewlett-Packard Systems Insight Manager	HP SIM 是統一伺服器與儲存管理平台。系統管理員可從單一的管理主控台使用安全管理工具組來管理其完整的 HP 伺服器與儲存環境。
ISEE	Instant Support Enterprise Edition	ISEE 是 Insight Remote Support Advanced 軟體的前身，已不再支援。
MC3	Remote Support 常用元件	MC3 針對傳輸至 HP 的事件提供唯一的識別資訊。
MVAA	Multi-Vendor and Application Adapter	MVAA 是軟體套件，可讓 Management Platform Synchronizer 支援 HP Operations Manager 與 Multi Vendor Support。您的 HP 客戶團隊可提供有關這些產品的額外資訊。
OSEM	Open Service Event Manager	OSEM 自 Insight Remote Support Advanced A.05.40 起停用，改用 WEBES 5.6。
RDC	Remote Device Collection	RDC 是透過 Remote Support 技術收集設定資訊，以提供主動式遠端支援服務的過程。
RDM	Remote Device Monitoring	RDM 是一個程序，可從受管理系統擷取硬體事件、在 CMS 篩選這些事件、透過 Insight Remote Support Advanced 將可能需要處理的事件提交給 HP，以及根據客戶支援授權的層級來爲這些事件提供支援。
RSCC	Remote Support Configuration Collector	RSCC 安裝在 CMS 上以處理 Configuration Data Collections。
RSCCE	Remote Support Configuration Collector Extension	RSCCE 能夠收集 SAN 服務的設定。
RSNC	Remote Support Network Component	支援有合約 HP 客戶的網路服務。
RSP	解決方案過去稱做 Remote Support Pack，現在稱做 Insight Remote Support Advanced	Insight Remote Support Advanced 可主動進行遠端監控、診斷與疑難排解，以協助提升您資料中心內 HP 所支援伺服器與儲存系統的可用性。HP Remote Support 可透過系統的支援來降低成本與複雜性。HP Remote Support 可將硬體事件資訊安全地通過您的防火牆和/或 Web proxy，傳遞至 HP 支援中心以進行反應式支援。此外會根據您支援服務合約的內容，決定是否收集系統資訊進行主動式分析與服務。
RSSWM	遠端支援軟體管理員	RSSWM 是 Insight Remote Support Advanced 解決方案的必要元件。它是經由 HP SIM 安裝在 CMS 上。
SFM	系統故障管理	SFM 是執行 WBEM 標準的 HP-UX 錯誤管理解決方案。系統故障管理與其他如 HP SIM、HP SMH 等容易管理的應用程式，和任何其他的 WBEM Client (例如 WEBES) 整合在一起。
SMH	System Management Homepage	SMH 是一種網頁式介面，可將 HP-UX、Linux 和 Windows 作業系統上的 HP 伺服器合併並簡化成單一系統管理。
SMS/SMA	儲存裝置管理伺服器或應用裝置	SMS/SMA 是安裝 HP StorageWorks Enterprise Virtual Array (EVA) 軟體的系統，包括 HP Command View EVA 與 HP Replication Solutions Manager (若有使用)。它是專用的管理系統，專門執行 EVA 管理軟體。
WBEM	Web Based Enterprise Management	基本上，WBEM 是業界的首創，可標準化不同平台間的管理資訊。
WEBES	Web-Based Enterprise Service	安裝在 CMS 上的 Remote Support 元件，可透過產品特定的規則集執行即時服務事件篩選。這些規則集會定期視是否有可用的改進功能予以更新。

排版慣例

find(1)	係指 HP-UX 線上援助頁。在此範例中，「find」 是線上援助頁的名稱而「1」 則是線上援助頁節數。
《書名 (Book Title)》	係指手冊或其他文件的標題，而楷書係指已中文化之手冊。
連結的標題	係指超連結連至書本或其他文件的標題。
http://www.hp.com	係指超連結至網站的網站位址。
命令 (Command)	係指命令名稱或有效的命令片語。
使用者輸入 **(UserInput)**	係指您鍵入的命令和其他文字。
電腦文字 (ComputerOut)	係指由電腦顯示的文字。
粗體大寫字 (Enter)	係指鍵盤按鍵的名稱。請注意，**Return** 與 **Enter** 係指同一個按鍵。如 **Ctrl+A** 的序列表示您必須同時按住標示為 **Ctrl** 的按鍵和 **A** 鍵。
辭彙 (Term)	係指重要文字或詞的定義使用。
變數 (Variable)	係指環境變數的名稱，例如 PATH 或 errno。
值 (value)	係指您可替換的值。該值在顯示的命令、函式或資訊中，代表數個可能值。
<元素>	係指用於標示 (markup) 語言內的一個元素 (element)。
屬性=	係指用於標示語言內的一個屬性。

相關與必要文件

如需其他 Insight Remote Support Advanced 資訊，請到： http://docs.hp.com/en/netsys.html#Remote Support Pack

表 1 支援文件

文件	必要或建議
《HP Systems Insight Manager Installation and Configuration Guide for Microsoft Windows》	必須在 CMS 上安裝與設定 HP SIM、SMH 和遠端支援軟體管理員 (RSSWM)。
地點： http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html#b2	
《Insight Remote Support Advanced 受管理系統手冊》	必要
地點： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《HP Insight Remote Support Advanced CMS 設定與使用手冊》	必要
地點： http://docs.hp.com/en/netsys.html#Remote Support Pack	

表 1 支援文件 (繼續)

文件	必要或建議
《A.05.40 Insight Remote Support Advanced Release Notes》	決定您受管理系統的支援性時必須使用。
地點： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《HP Remote Support Software Manager Configuration, Usage and Troubleshooting Guide for Insight Remote Support Advanced》	只有在您要修改 Insight Remote Support Advanced 套件與 RSSWM 工具本身的設定時才需要。
地點： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《遠端支援軟體管理員 A.05.40 升級指南》	只有在您是從上一版 Insight Remote Support Advanced 升級時才需要。新安裝記錄在《HP Systems Insight Manager Installation and Configuration Guide for Microsoft Windows》中。
地點： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《EVA CommandView 安裝指南》	只有在您安裝 Insight Remote Support Advanced 以監控 EVA 裝置時才需要。
地點： http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c01681292/c01681292.pdf	
HP Insight Management WBEM Providers 網站	請參閱 WBEM 供應商網站以取得 WBEM 供應與與認證的詳細資訊。
地點： http://h18013.www1.hp.com/products/servers/management/wbem/documentation.html?jumpid=reg_R1002_USEN	
《HP WEBES Reference Guide》	有關 System Event Analyzer (SEA) 使用者介面的詳細資訊。
地點： http://h18023.www1.hp.com/support/svctools/webes/index.html	
《HP WEBES Installation, Configuration, and Usage Guide》	如果您在安裝 Insight Remote Support Advanced 元件之前，遇到無法移除舊版 HP WEBES 或 WCCProxy 的狀況，建議您參閱此手冊。
地點： http://h18023.www1.hp.com/support/svctools/webes/index.html	

表 1 支援文件 (繼續)

文件	必要或建議
《HP-UX 系統故障管理指南》	如果您目前無法達到 SFM 最低需求，而無法獲得 HP-UX 受管理系統的支援，如《Insight Remote Support Advanced 受管理系統手冊》中定義，則建議使用。
地點： http://docs.hp.com/en/5992-6257/5992-6257.pdf	

1 Insight Remote Support Advanced：受管理系統概觀

1.1 瞭解受管理系統使用前提

若要使用 Insight Remote Support Advanced，您至少需要兩種硬體：一個相容的 Windows ProLiant 裝置作爲中央管理伺服器 (CMS) 和至少一個受管理系統。 必須確認您的受管理系統眞的可以管理，才能開始使用 Insight Remote Support Advanced。本《`Insight Remote Support Advanced 受管理系統手冊`》 文件提供在您的 CMS 上安裝和設定 Insight Remote Support Advanced 軟體之前，確認是否已正確設定硬體的必要資訊。

1.1.1 受管理系統上的通訊協定

受管理系統可以使用下列一或多種通訊協定來與 CMS 進行通訊：

- SNMP
- WBEM
- ELMC

適當的通訊協定取決於受管理系統類型和所需的通訊。請閱讀本文中適當的受管理系統章節，以瞭解您的特定受管理系統需要什麼樣的設定。

在某些情況下，可能需要多種通訊協定。這是因爲 CMS 上的 HP SIM 可能會使用某些通訊協定來尋找受管理系統，而其他通訊協定可能會用來監視硬體事件或從受管理系統擷取資料收集資訊。下表特別指出需求，但您必須閱讀內容適合您的受管理系統類型的受管理系統章節，以取得更詳細的資訊。

表 1-1 您受管理系統的必要資訊

受管理系統類型	裝置探索	硬體事件的遠端監視	遠端資料收集
Windows ProLiant	SNMP 或 WBEM	SNMP 或 WBEM	SNMP 或 WBEM
ProLiant Linux	SNMP 或 WBEM	SNMP 或 WBEM	SNMP 或 WBEM
Integrity Linux	WBEM	WBEM	WBEM
Integrity Windows 2003	WBEM	ELMC	WBEM
Integrity Windows 2008	WBEM	WBEM	WBEM
HP-UX	WBEM (SFM)	WBEM (SFM)	WBEM (SFM)
OpenVMS	ELMC	ELMC	ELMC
Tru64 Unix	ELMC	ELMC	ELMC
SanSwitch 和磁帶櫃	SNMP	SNMP	SNMP
目標型 MSA	SNMP	SNMP	SNMP
EVA	SNMP 或 WBEM	ELMC	CommandView for EVA

1.2 受管理系統建議

1.2.1 一般建議



附註： 使用 WBEM 認證來監視受管理系統時，如果您變更使用者名稱/密碼，不論是否因爲認證太舊或過期而自動變更，還是您在維護時手動變更它們，您都「必須」在 CMS 上的 HP SIM 中修改這些認證，才能繼續監視受管理系統。

下列建議是針對本文未涵蓋或未完全涵蓋的受管理系統類型

- 如需多供應商或多平台的支援，請連絡 HP 客戶小組成員，以取得相關資訊。

- 若為 NonStop 系統，請參閱本文的 Windows Integrity 章節。



附註： Open System Management (OSM) T0682 SPR H02 ABU 是特別針對 NonStop 支援的一項受管理系統需求。

CMS 還有其他特別針對 NonStop 支援的軟體需求。如需詳細資訊，請參閱《HP Insight Remote Support Advanced CMS 設定與使用手冊》。

1.3 收集必要的受管理系統資訊



附註： 請利用下表來記錄您每一個受管理系統的相關資訊。在您設定 CMS 時將會用到這項資訊，此外，您也可能需要此資訊來確認您的受管理系統是否相容且可搭配 Insight Remote Support Advanced 一起使用。

表 1-2 您受管理系統的必要資訊

必要項目	值
完整主機名稱	
IP 位址	
要在此受管理系統上使用的 WBEM 帳戶名稱	
地點 (受管理系統的實際位置)	
序號	
產品編號	
SAID 或系統控制編號	
主要支援服務聯絡人	
主要連絡人的電話號碼	
主要連絡人的電子郵件地址	
主要連絡人的可連絡時間	
其他連絡人的電話號碼	
其他連絡人的電子郵件地址	

1.4 關於本文件

《A.05.40 Insight Remote Support Advanced Release Notes》(可於 http://docs.hp.com/en/netsys.html#Remote Support Pack 上取得) 中說明支援的受管理系統的硬體和作業系統規格。

相對應的章節中詳細說明受管理系統遠端支援的特定軟體和設定需求。



重要： 如果您將不會監視下列任何一種受管理系統類型，受管理系統章節的編排方式可讓您直接跳過那一章。

- 第 2 章「設定主控 Windows 的 ProLiant 受管理系統」
- 第 3 章「設定適用於 ProLiant Linux 受管理系統的 SNMP 支援」
- 第 4 章「設定主控 VMware ESX-i 的 ProLiant 受管理系統」
- 第 5 章「設定主控 VMware ESX 的 ProLiant 受管理系統 」
- 第 6 章「Linux Integrity 受管理系統使用前提」
- 第 7 章「Windows Integrity Server 受管理系統使用前提」
- 第 8 章「NonStop 受管理系統的安裝與設定」

- 第 9 章「Insight Remote Support 的 HP-UX 受管理系統需求」
- 第 10 章「OpenVMS 受管理系統的 Insight Remote Support Advanced 支援使用前提」
- 第 11 章「可獲得 Insight Remote Support Advanced 支援之 Tru64 Unix 受管理系統的需求」
- 第 12 章「HP Insight Remote Support Advanced 的 EVA 支援需求 」
- 第 13 章「適用於 Insight Remote Support Advanced 支援之 San Switch 與磁帶櫃的需求」
- 第 14 章「使用目標型 SNMP 支援來設定 MSA 受管理系統」

1.5 檢閱受管理系統傳送的測試事件

某些受管理系統類型允許您將測試事件、trap 或指示傳送給 CMS。在您設定受管理系統並將測試事件傳送給 CMS 後，請使用下列程序來找到 CMS 上的測試事件、trap 或指示。

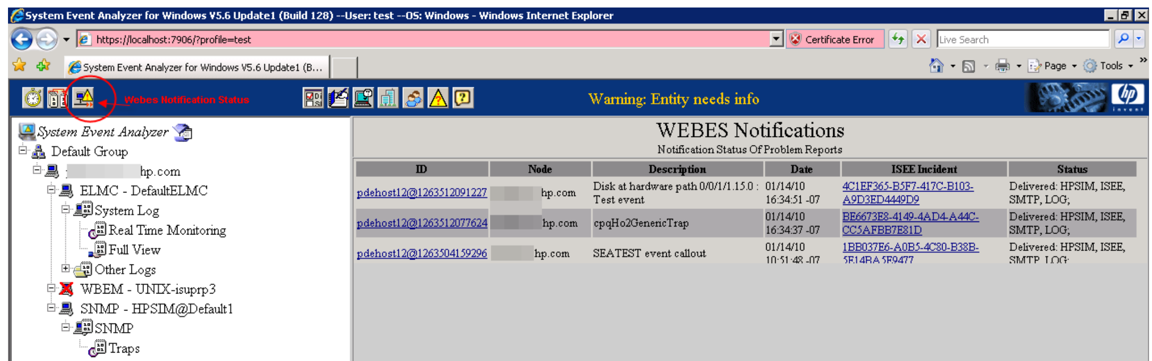
1. 登入 System Event Analyzer (SEA)：
   a. 按一下 **[開始]** → **[所有程式]** → **[Hewlett-Packard Service Tools]** → **[System Event Analyzer]** → **[System Event Analyzer]**。



附註： 如果您是從其他系統登入 CMS，請開啓 Web 瀏覽器，然後輸入下列 URL：
`https://localhost:7906`
如果您無法使用 `localhost`，請改用 CMS 的完整主機名稱或 IP 位址。

   b. 系統將提示您輸入此工作階段的設定檔使用者名稱，這可以是您選擇的任何名稱。輸入名稱，然後按一下 **Logon**。
   c. 如果瀏覽器提示您該站點沒有已簽署的憑證，請按一下可讓您繼續前往該網頁的連結。此應用程式是裝載於 CMS 上。

2. 在 SEA 介面中，按一下 **WEBES Notification Status** 圖示 (請參閱下列影像中圈起來的圖示)。



3. 若您已正確設定受管理系統並已傳送測試事件，該測試事件應該會顯示在 SEA 的輸出上。

2 設定主控 Windows 的 ProLiant 受管理系統

您必須先進行下列動作，才能監視 Windows ProLiant 受管理系統：

- 藉由查看《`A.05.40 Insight Remote Support Advanced Release Notes`》來驗證您的受管理系統是否受到支援。
- 從您的受管理系統中移除任何舊版或相衝突的 Remote Support 軟體。
- 確認您的ProLiant受管理系統上已安裝SNMP (如果您慣用SNMP)。HP建議您安裝Windows SNMP OS 支援套件。
- 確認您的受管理系統上已安裝並設定正確的 ProLiant Support Pack (PSP) 工具。如果您使用的是 WBEM，請確認已正確設定 IM Providers。
- 測試從受管理系統到 CMS 的連線。

2.1 從 Windows ProLiant 受管理系統移除相衝突的軟體

下列各小節將提供從受管理系統移除舊版 Remote Support 軟體應用程式所需的步驟。

2.1.1 移除 HP ISEE

「唯有」當您在受管理系統上已安裝 HP Instant Support Enterprise Edition (ISEE) 時，才需要進行這些步驟。如果您沒有在受管理系統上安裝 ISEE，可以跳過這一節。



重要： Instant Support Enterprise Edition (ISEE) A.03.95 及舊版與 Insight Remote Support Advanced「不是相同的應用程式」，請不要安裝在任何含有 Insight Remote Support Advanced 的系統上。

若要移除 ISEE，請執行下列步驟：

1. 在控制台中，連按兩下 **[新增/移除程式]**。
2. 在 **[新增/移除程式]** 對話方塊中，找出 ISEE 項目 (如果有的話)，然後按一下 **[移除]**。

2.1.2 移除 WEBES



附註： 移除 ISEE 之後，如果移除 WEBES，應該也會一併移除 WCCProxy。如果未移除 ISEE，則 WEBES 不會移除 WCCProxy。



秘訣： 在移除 WEBES 之前，建議您存取 System Event Analyzer (SEA) UI，並從 Managed Entities 頁面中找回系統序號和產品 ID。之後當您在 CMS 的 HP Insight Remote Support 中設定受管理系統的內容時，此資訊就可以派上用場。

若要解除安裝所有 WEBES 工具 (包括 WCCProxy)，請依照下列步驟執行：

1. 使用具備系統管理員權限的帳戶登入受管理系統。
2. 將所有正在執行的工具全部關閉。
3. 在控制台中，連按兩下 **[新增/移除程式]**。
4. 在 **[新增/移除程式]** 對話方塊中，找出 WEBES 項目並按一下 **[變更/移除]**，以執行安裝精靈。
5. 出現提示時，選擇 **Remove** 選項。
6. 依照提示來執行解除安裝。
7. 在 **[新增/移除程式]** 對話方塊中，確認沒有 WCCProxy 項目。如果有這個項目，您可以選取它並按一下 **[移除]**，手動將它移除。

2.1.3 移除 OSEM

解除安裝將會完全移除 OSEM 目錄下的所有檔案。如有需要，您可以手動備援設定檔案，例如 `working.props`、`hosts.txt` 或 `communities.txt`。

您可能也想要備援通知資料夾，以保留所有問題報告的複本。OSEM 1.3.7 或以上版本在解除安裝過程中會建立所有設定和狀態資訊的複本。

若要解除安裝所有 OSEM 工具，請依照下列步驟執行：

1. 使用具有系統管理員權限的帳戶登入。
2. 將所有正在執行的工具全部關閉。
3. 在控制台中，連按兩下 **[新增/移除程式]**。
4. 在 **[新增/移除程式]** 對話方塊中，找出 OSEM 項目並按一下 **[移除]**，以執行安裝精靈。



小心： 在安裝精靈中，第一個 **Cancel** 是您徹底結束解除安裝常式的唯一機會。之後，即使有取消或結束選項可用，也不要再取消或停止解除安裝。

5. 遵循提示繼續解除安裝。

2.1.4 關於 ProLiant Support Pack (PSP)

ProLiant Support Pack (PSP) 是一個系統專屬的軟體組合，其中包括適用於 ProLiant 裝置的驅動程式、公用程式及管理代理程式。PSP 隨附於 HP SmartStart CD 上的每套 ProLiant 中。您也可以在 www.hp.com/servers/psp 上取得最新版本。



附註： PSP 安裝預設會使用 SNMP，WMI 則是選擇的項目。

2.1.4.1 Windows 的 IM Providers 或 IM Agents

執行 MS Windows 的 HP ProLiant 系統都受到 Insight Management Providers (適用於 WBEM/WMI Mapper 的 IM Providers 支援) 或 Insight Management Agents (適用於 SNMP 的 IM Agents 支援) 的支援。提供者與代理程式都可以透過相同的 PSP 媒體來取得。對於 Insight Remote Support Advanced，在 SmartStart CD 上和/或 ProLiant Support Pack (PSP) 8.1 版或更高版本中的 IM Providers 都受到支援。

如需 WBEM 提供者、安全性及認證的詳細資訊，請參閱HP Insight Management WBEM Providers 網站，網址爲 http://h18013.www1.hp.com/products/servers/management/wbem/documentation.html?jumpid=reg_R1002_USEN。

如果 SNMP 和 WBEM 都可以在 Windows Proliant 受管理系統上取得，則建議您在 HP SIM 上停用其中一個通訊協定的監視功能，以防止在發生單一受管理系統故障時收到雙重通知。如果沒有任何像是 MSA 的智慧型卸離儲存裝置已連接到受管理系統，請停用 SNMP。如果已安裝智慧型卸離儲存裝置，則請在 HP SIM 中停用 WMI 通訊協定。您可以在 HP SIM 中編輯受管理系統，然後從適用於該通訊協定的下拉式方塊中選取 **off**，來完成此作業。

如果使用的是 Windows SNMP Agents (IM Agents)，就必須設定 SNMP 以便與 CMS 進行通訊。本章所提供的就是適用於該設定的指示。

如果使用的是 Windows WBEM Providers (IM Providers)，並且您隨時都會變更 WBEM 認證 (不論是手動或自動)，就必須在 CMS 的 HP SIM 使用者介面中修改這些認證項目。此程序的指示記錄於《HP Insight Remote Support Advanced CMS 設定與使用手冊》中。此外，您必須在 CMS 上使用 HP SIM 來設定每個受管理系統的 WBEM 認證，才能監視他們。



附註： WBEM IM Providers 在 ProLiant Support Pack 安裝中是選擇的項目。請確定您在安裝 PSP 時有選取這些項目。

2.1.4.2 System Management Homepage

System Management Homepage (SMH) 也是 PSP 的一部分，它會在受管理系統本身上提供其他的報告功能。由於對 Insight Remote Support Advanced 並非必要，所以如果您未在安裝 Insight

Management Agent 期間正確設定 SNMP 服務以便與 CMS 進行通訊，則可使用 SMH 重新設定這些設定。如果您已在安裝 ProLiant Support Pack (PSP) 的同時安裝了預設的 SNMP 設定和選擇的 WMI 設定，則 SMH 將預設為 WMI 設定，而且如果您選擇透過 SNMP 來取得硬體事件，則可能需要將其重設為 SNMP。



附註： 根據預設，SMH 會與 HP Insight Remote Support Solution 一起安裝在 CMS 上。

2.1.5 在 Windows ProLiant 受管理系統上設定 SNMP

您的受管理系統必須設定為可與 CMS 進行通訊。如果您選擇使用 SNMP，則需執行下列步驟，才能讓受管理系統可與 CMS 進行完整通訊。

參與 SNMP 通知的受管理系統必須包含下列項目：

- 所有受管理系統都必須具備已安裝並執行 TCP/IP 的作用中內部網路連線 (例如，透過乙太網路介面卡)。受管理系統必須透過此連線來與 CMS 進行雙向通訊。
- 受管理系統需要 Insight Management Agent 軟體來偵測問題及產生 trap。IM Agents 是由 HP 所發佈，其設計目的是產生含有可進行更完整分析之資訊的 SNMP trap。
- 最後，所有的受管理系統都必須定義傳送 trap 目的地之 CMS 主機的 IP 位址。

2.1.5.1 Windows 受管理系統 SNMP 設定

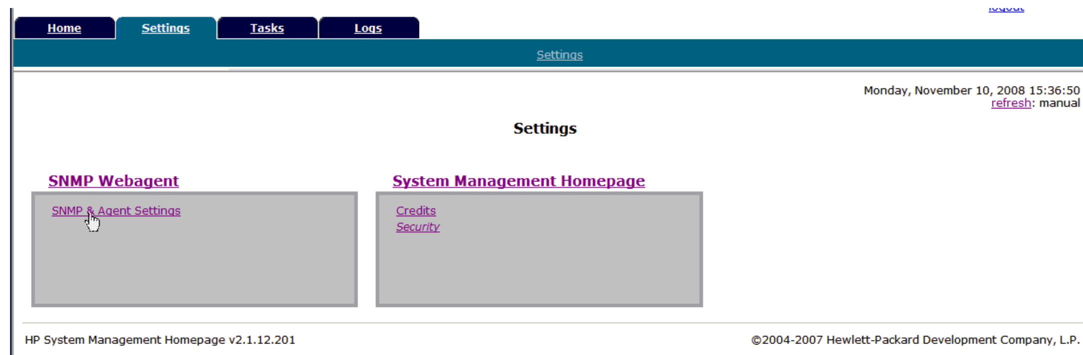
CMS 必須能夠與受管理系統進行通訊，但是根據預設，Windows Server 2003 只接受來自 localhost 的 SNMP 封包。若要設定 Windows Server 2003 將 trap 傳送至 CMS：

1. 使用 Web 瀏覽器存取受管理系統上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管理系統的系統管理員使用者名稱和密碼進行登入。



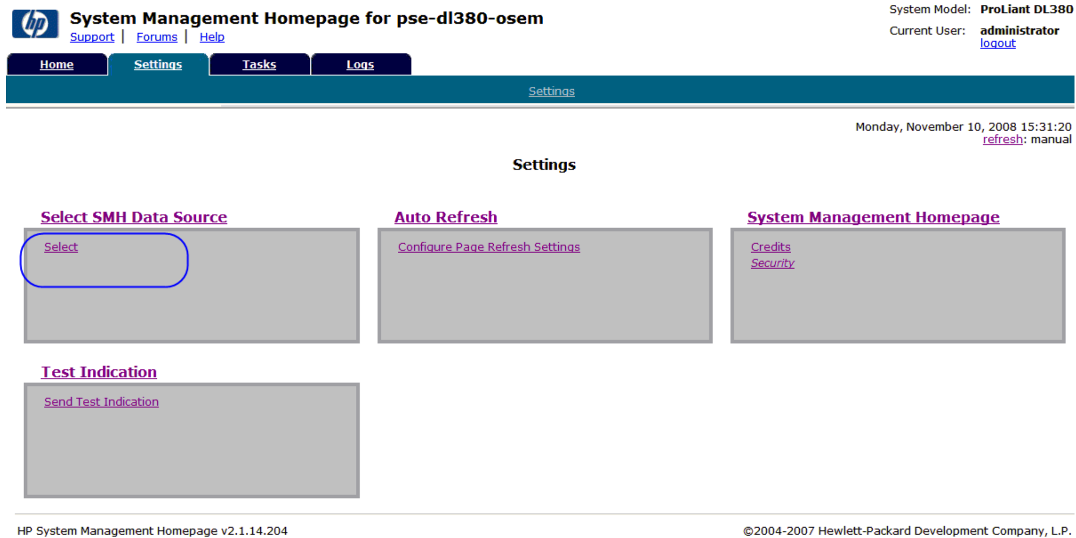
附註： 如果系統並未提示您登入，請檢查 SMH 介面的右上角，並按一下 **Sign In** 連結。如果沒有以系統管理員身分登入受管理系統，您將不會擁有所有的相關設定選項。

3. 按一下 **Settings** 標籤/選項。

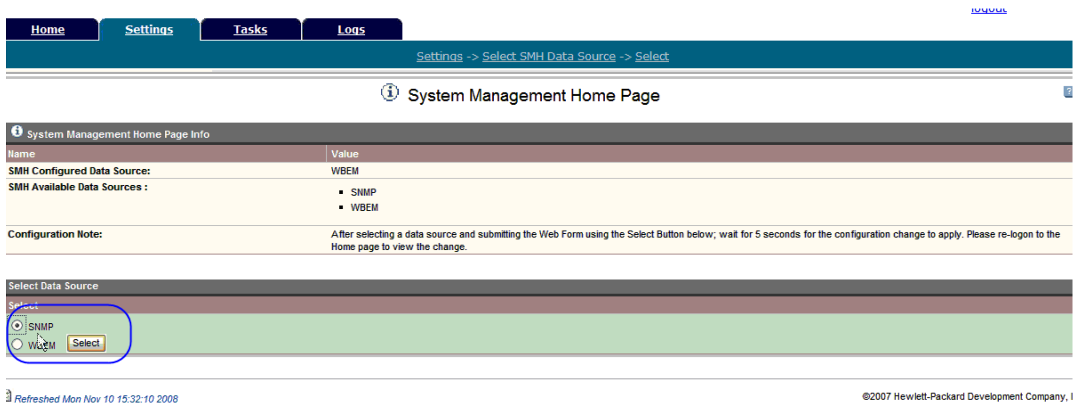




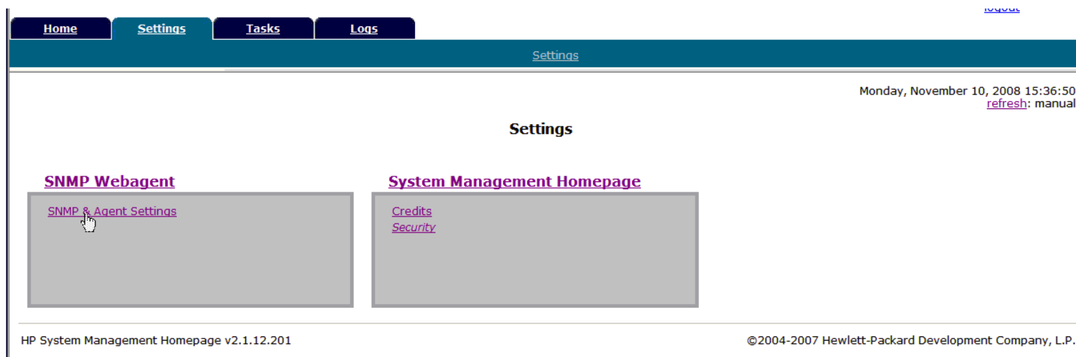
重要： 如果 **Settings** 標籤未顯示上述影像，但顯示了下列影像，則請在 **Select SMH Data Source** 方塊中，按一下 **Select** 連結。



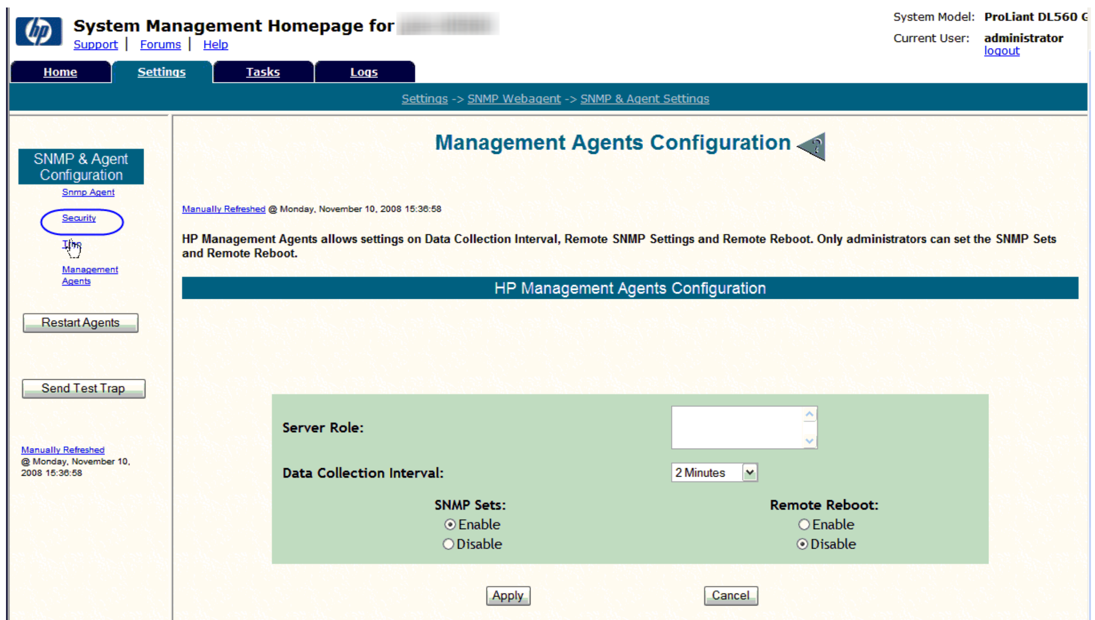
若已在這個受管理系統上設定 WBEM/WMI Providers，則可能需要切換成 SNMP 設定 (請參閱下列影像)。如果需要切換，可將圓鈕切換成 SNMP，然後按一下 **Select**。如果在您從遠端登入受管理系統上的 SMH 時發生此狀況，則必須再次登入，並回到 **Settings** 標籤。



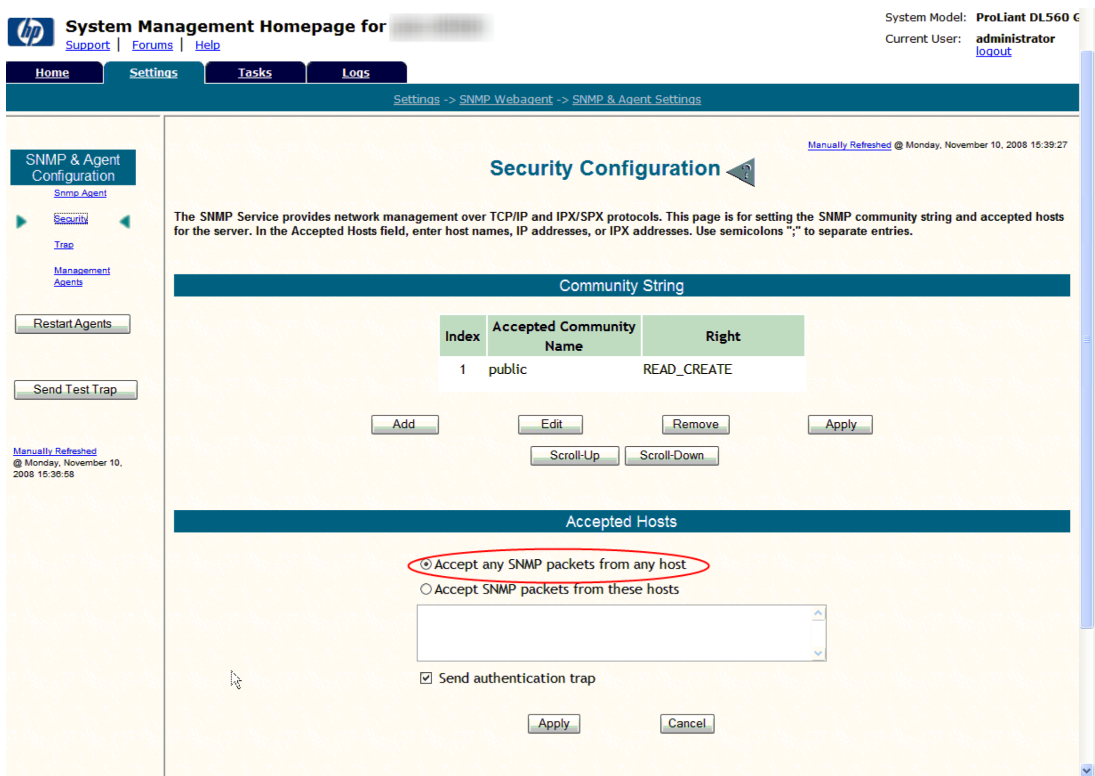
4. 在 **SNMP Web Agent** 方塊中，按一下 **SNMP and Agent** 連結。



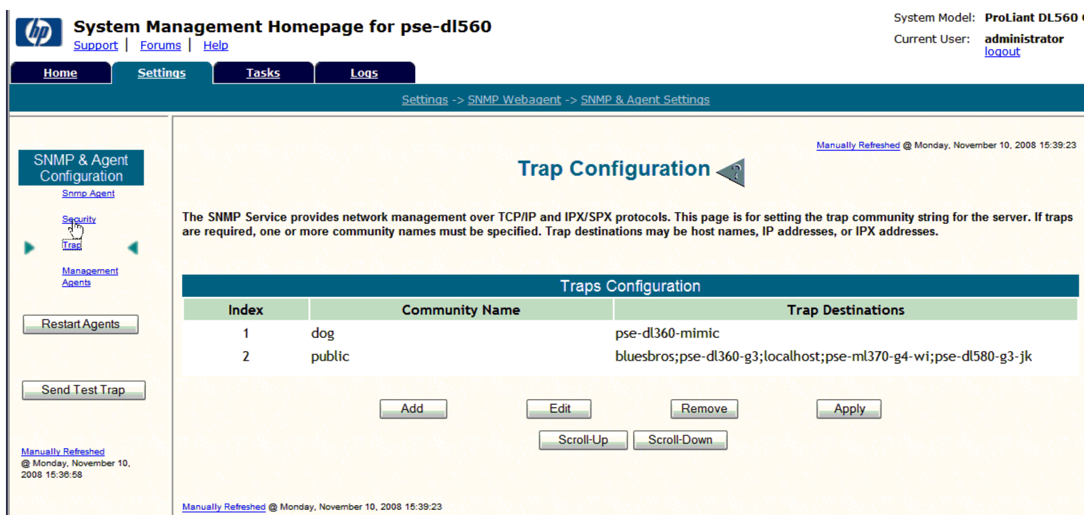
5. 在 Management Agent Configuration 畫面的左側導覽清單中，按一下 **Security** 連結。



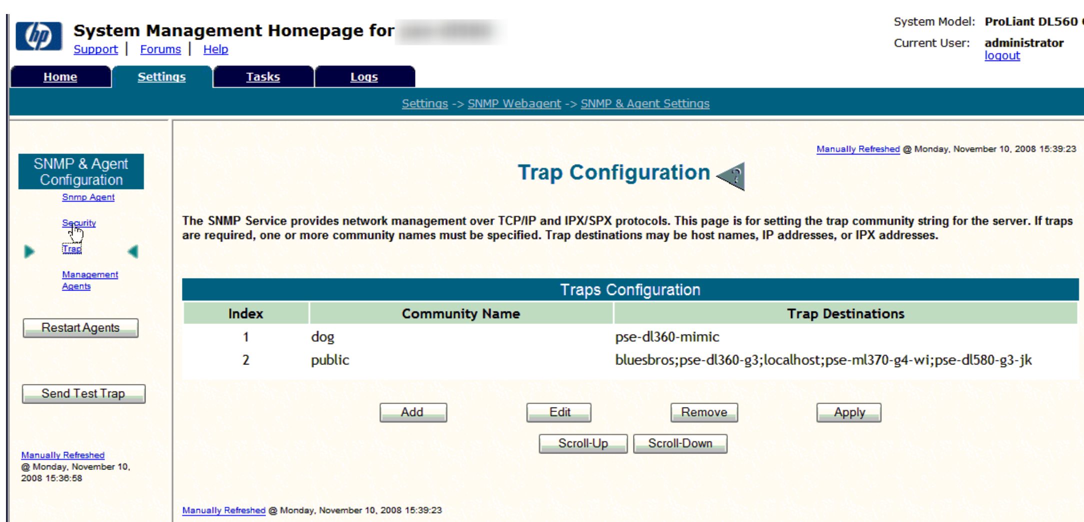
6. 在 Security 畫面中，您可以在 **Accept SNMP packets from these hosts** 選項中指定 CMS 的 IP 位址，或者只選取 **Accept SNMP packets from any host** 選項。



7. 在 Security 畫面左側，按一下 **Traps** 連結。



8. 在 **Trap Configuration** 畫面中，新增將會包含 CMS 的社群字串，或者編輯公用字串以包含 CMS。





附註： 您將需要針對每個要透過 SNMP 與 CMS 通訊的 Windows ProLiant 受管理系統，完成前述步驟。

2.2 傳送測試至 CMS

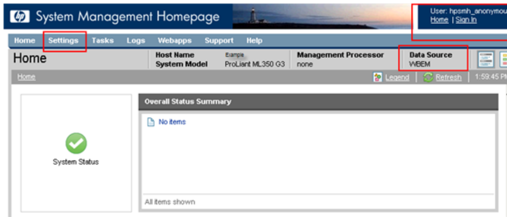
2.2.1 傳送 WBEM 測試指示

1. 使用 Web 瀏覽器存取受管理系統上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管理系統的系統管理員使用者名稱和密碼進行登入。

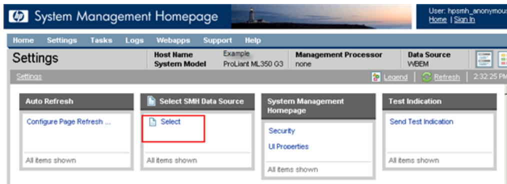


附註： 如果系統並未提示您登入，請檢查 SMH 介面的右上角，並按一下 **Sign In** 連結。如果沒有以系統管理員身分登入受管理系統，您將不會擁有所有的相關設定選項。

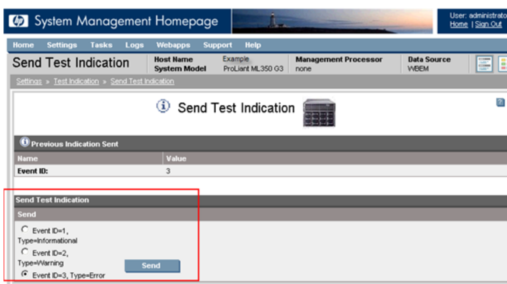
3. 按一下 **Settings** 選項。



4. 如果您選擇利用 ProLiant Support Pack 來安裝 WBEM，其將設定為您的資料來源，請按一下 **Send Test Indication** 選項。



在 **Send Test Indication** 視窗中，選取事件 ID 類型 (任何可運作的類型)，然後按一下 **Send** 按鈕。

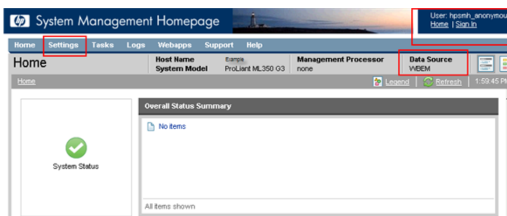


2.2.2 傳送 SNMP 測試 trap

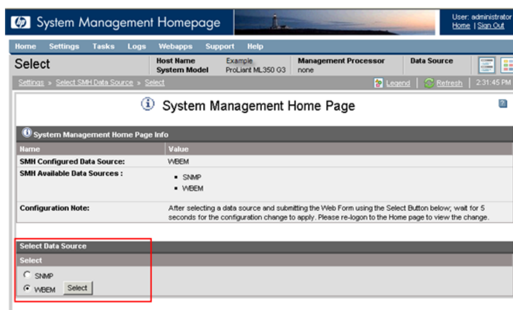
1. 使用 Web 瀏覽器存取受管理系統上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管理系統的系統管理員使用者名稱和密碼進行登入。

 **附註：** 如果系統並未提示您登入，請檢查 SMH 介面的右上角，並按一下 **Sign In** 連結。如果沒有以系統管理員身分登入受管理系統，您將不會擁有所有的相關設定選項。

3. 按一下 **Settings** 選項。



4. 如果您選擇利用 ProLiant Support Pack 來安裝 WBEM，其將會設定為您的資料來源。如果是這樣，若要使用 SNMP，可以按一下 **Select SMH Data Source** 標題下方的 **Select** 選項以變更為 SNMP。



在 Data Source 選項功能表中，選擇 **SNMP** 圓鈕，然後按一下 **Select** 按鈕。

5. 一旦將 Data Source 設定爲 SNMP 之後，可以按一下 **Settings** 選項，然後選取 **SNMP & Agent Configuration** 設定。
6. 在 **Management Agents Configuration** 視窗中，按一下 **Send Test Trap** 按鈕。

如需有關檢閱測試指示或 trap 的詳細資訊，請參閱「檢閱受管理系統傳送的測試事件」。

3 設定適用於 ProLiant Linux 受管理系統的 SNMP 支援

您必須先進行下列動作，才能使用 SNMP 來監視 ProLiant 受管理系統：

- 查看《`A.05.40 Insight Remote Support Advanced Release Notes`》，確認該系統是支援的系統。
- 確認已移除舊版的 Remote Support 工具 (如果適用)。
- 確認已在系統上安裝並設定正確的 ProLiant Support Pack (PSP) 工具。



附註： 對於支援的 Linux ProLiant，您必須先從 PSP 安裝 (或確認是否已經安裝) IM Agents 7.1 版或更高版本，才能繼續進行。SNMP 支援 (包括 IM Agents 和 Health Drivers) 無法在與 WBEM (包括 IM Providers 和 Health Drivers) 相同的受管理系統上受到支援。如果您計劃支援這個含 SNMP 的受管理系統，則必須根據 ProLiant Support Pack 說明文件來移除 WBEM 支援功能 (如已安裝)。

- 確認您的 Linux ProLiant 受管理系統上已安裝並正確設定 SNMP
- 測試從受管理系統到 CMS 的通訊

3.1 從 Linux ProLiant 受管理系統移除相衝突的軟體

3.1.1 從 Linux ProLiant 受管理系統中移除 HP ISEE

1. 關閉任何正在執行 ISEE Client 使用者介面的瀏覽器。
2. 以 root 身分 (系統管理權限) 登入受監視系統。
3. 切換至您安裝 HP ISEE 時所建立的目錄 (cd)。



附註： 此目錄名稱列在 `/opt/hpservices/RemoteSupport/config/installDir` 中

4. 若要從受監視系統中移除 HP ISEE 軟體，請執行下列指令：

   ```
   bash uninstall.sh
   ```

3.1.2 從 Linux ProLiant 受管理系統中移除 WEBES

使用互動式公用程式是移除整個 WEBES 套件最輕鬆的方法：

1. 執行下列指令來執行互動式工具：

   ```
   /usr/sbin/webes_install_update utility
   ```

2. 選擇 *移除所有* WEBES 的選項
3. 依照任何出現的提示進行。

3.2 在受管理系統上設定 SNMP

您的 Linux 受管理系統必須設定為可與 CMS 進行通訊。

參與 SNMP 通知的受管理系統必須包含下列項目：

- 所有受管理系統都必須具備已安裝並執行 TCP/IP 的作用中內部網路連線 (例如，透過乙太網路介面卡)。受管理系統必須透過此連線來與 CMS 進行雙向通訊。
- 受管理系統需要 Insight Management Agent 軟體來偵測問題及產生 trap。IM Agents 是由 HP 所發佈，其設計目的是產生含有可進行更完整分析之資訊的 SNMP trap。
- 最後，所有的受管理系統都必須定義傳送 trap 目的地之 CMS 主機的 IP 位址。

3.2.1 關於 ProLiant Support Pack (PSP)

ProLiant Support Pack (PSP) 是一個系統專屬的軟體組合，其中包括適用於 ProLiant 裝置的驅動程式、公用程式及管理代理程式。PSP 隨附於 HP SmartStart CD 上的每套 ProLiant 中。您也可以在 www.hp.com/servers/psp 上取得最新版本。

3.2.1.1 適用於 Linux 的 IM Agents

執行 Linux 的 HP ProLiant 系統均受到 Insight Management Agents (IM Agents) 所支援，而這些代理程式也可以透過 PSP 來傳遞。對於 Insight Remote Support，在 SmartStart CD 和/或 ProLiant Support Pack (PSP) 7.1 版或更高版本中的 IM Agents 均受到支援。



附註： 在您的 Linux 受管理系統上， `/etc/snmp/snmpd.conf` 檔案會包含目前的 SNMP 設定。在設定 IM Agents 的安裝指令碼期間，請觀看此檔案的相關資訊。當指令碼提示您有關從遠端管理站設定 SNMP 存取的資訊時，請確定會包含您 CMS 的 IP 位址。若未包含，則需在受管理系統上重新設定此 IP 位址。

3.2.1.2 System Management Homepage

System Management Homepage (SMH) 也是 PSP 的一部分，它會在受管理系統本身上提供其他的報告功能。由於對 Insight Remote Support Advanced 並非必要，所以如果您未在安裝 Insight Management Agent 期間正確設定 SNMP 服務以便與 CMS 進行通訊，則可使用 SMH 重新設定這些設定。

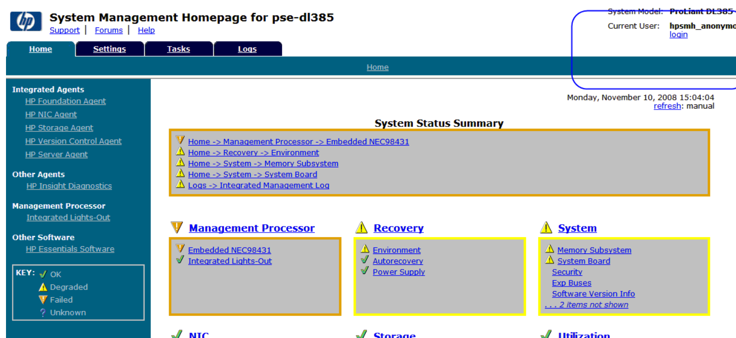


附註： 根據預設，SMH 會與 HP Insight Remote Support Solution 一起安裝在 CMS 上。

3.2.2 Linux 受管理系統 SNMP 設定

如前所述， Insight Management Agents 對 Linux 受管理系統而言是必要的。一旦將 Insight Management Agents 安裝至受管理系統之後，您便可存取 `snmpd.conf` 檔案，為來自受管理系統的 SNMP 通訊新增 CMS 的 IP 位址。您需要針對每個 Linux 受管理系統執行此動作。

1. 使用 Web 瀏覽器存取受管理系統上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管理系統的 root 使用者名稱和密碼進行登入。



3. 按一下 **Settings** 標籤。

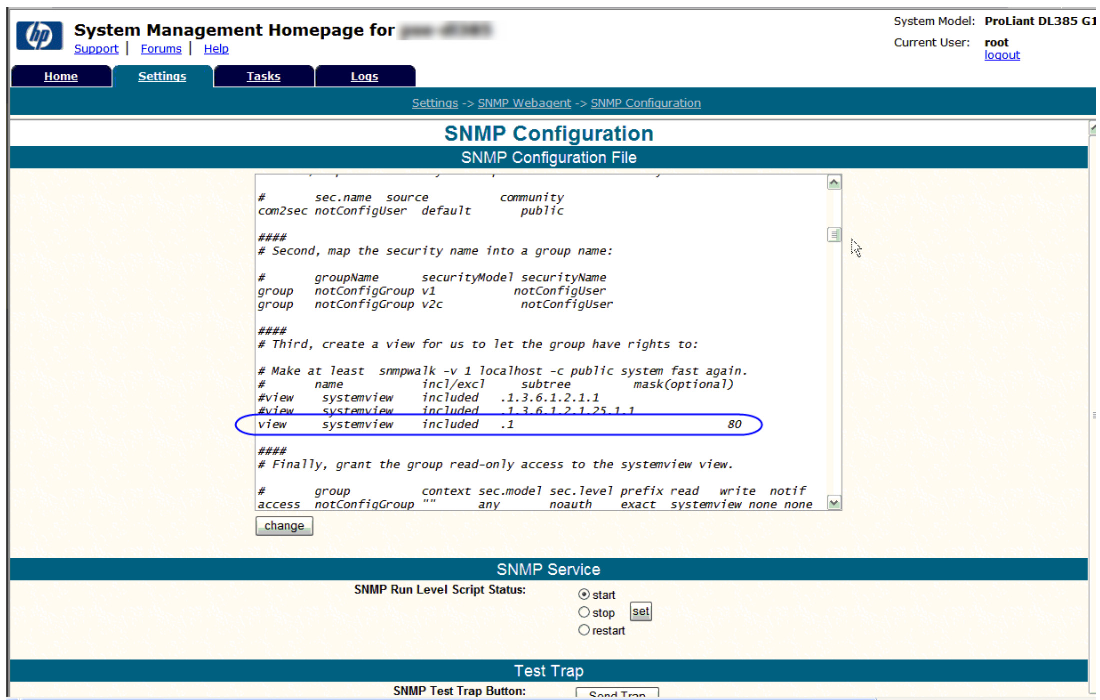
4. 按一下 **SNMP Configuration** 連結。
5. 在 **SNMP Configuration File** 中，新增 `trapsink` 指令，以包含 CMS 的 IP 位址 (例如，`trapsink 1.2.3.4 public`)，然後按一下 **Change**。



附註： 對於這些支援新增檢視陳述式之安全性的 Linux 安裝 (例如，Red Hat 4 或 5)，則應從預設值中進行下列調整。如果您沒有將 trapsink 項目指定為 public，則必須為這個受管理系統，以及 CMS 上任何其他透過 HP SIM 使用相同社群字串的系統，設定新的 SNMP 通訊協定。

6. 對於能夠收集所有關於此受管理系統之相關資訊的 CMS，您需要在 **SNMP Configuration File** 中向下捲動至 `view systemview included` 項目。將含有 # 字元的預設項目取消註解，然後新增此項目：

   `view systemview included .1 80`，接著按一下 **Change**。





附註： 如果您並未使用 SMH，也可以藉由在文字編輯器中編輯 snmpd.conf 檔案來執行此動作。

3.3 將 SNMP 測試 trap 傳送至 CMS

您可以遵循「Linux 受管理系統 SNMP 設定」中的說明，並且在 **Settings** 標籤上按一下 **Send Trap** 來使用 SMH 介面。但是，您也可以輸入下列指令，將測試 trap 發送至 CMS。

```
snmptrap -v1 -c public CMS IP Address.1.3.6.1.4.1.232 Linux Manage
System IP Address 6 11003 1234 .1.3.6.1.2.1.1.5.0 s test
.1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0 s "provide
your own identifiable identifier and time stamp"
```

此時應該會傳回含有受管理系統和 CMS 之詳細資料的結果文字。

```
Management Agents Test Trap sent - [timestamp]
```

如需有關檢閱測試指示或 trap 的詳細資訊，請參閱「檢閱受管理系統傳送的測試事件」。

4 設定主控 VMware ESX-i 的 ProLiant 受管理系統

您必須先進行下列動作，才能監視 ESX-i ProLiant 受管理系統：

- 查看《`A.05.40 Insight Remote Support Advanced Release Notes`》，確認該系統是支援的系統。
- 根據製造商的指示來驗證是否已設定 ESX-i 系統。如果已正確設定，則可使用所有需要的 WBEM 提供者。

4.1 關於 VMware ESX-i 與 Insight Remote Support Advanced

VMware ESX-i (已正確且完整安裝時) 將包含所需的 WBEM 提供者，以便與 CMS 進行有關硬體事件的通訊。ESX-i 系統的 root 帳戶認證將是您在 CMS 上設定此受管理系統之 WBEM 通訊協定時需使用的認證。由於 ESX-i 中不具備 System Management Homepage 功能，因此不提供目前可從受管理系統執行至 CMS 的 WBEM 指示。

5 設定主控 VMware ESX 的 ProLiant 受管理系統

您必須先進行下列動作，才能監視 ESX ProLiant 受管理系統：

- 藉由查看《`A.05.40 Insight Remote Support Advanced Release Notes`》來驗證您的受管理系統是否受到支援。
- 確認您的 ProLiant 受管理系統上已正確設定 SNMP

5.1 在 ESX 受管理系統上設定 SNMP

您的受管理系統必須設定為可與 CMS 進行通訊。VMware ESX 會使用 SNMP 來與 CMS 進行通訊。根據預設，SNMP 會與 VMware ESX 一同安裝，但是您必須設定受管理系統 SNMP，才能與 CMS 進行通訊。

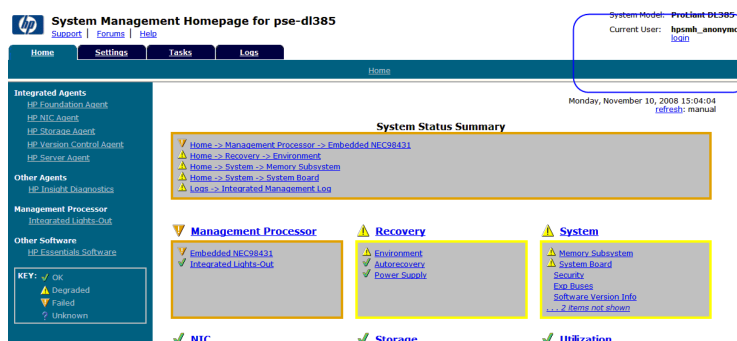
參與 SNMP 通知的受管理系統必須包含下列項目：

- 所有受管理系統都必須具備已安裝並執行 TCP/IP 的作用中內部網路連線 (例如，透過乙太網路介面卡)。受管理系統必須透過此連線來與 CMS 進行雙向通訊。
- 受管理系統需要 Management Agent 軟體來偵測問題及產生 trap。IM Agents 是由 HP 所發佈，其設計目的是產生含有可進行更完整分析之資訊的 SNMP trap。利用 VMware ESX，管理代理程式均為 VMware ESX 組合的一部分。因此，若您已正確設定受管理系統，代理程式即會出現在系統上。
- 最後，所有的受管理系統都必須定義傳送 trap 目的地之 CMS 主機的 IP 位址。

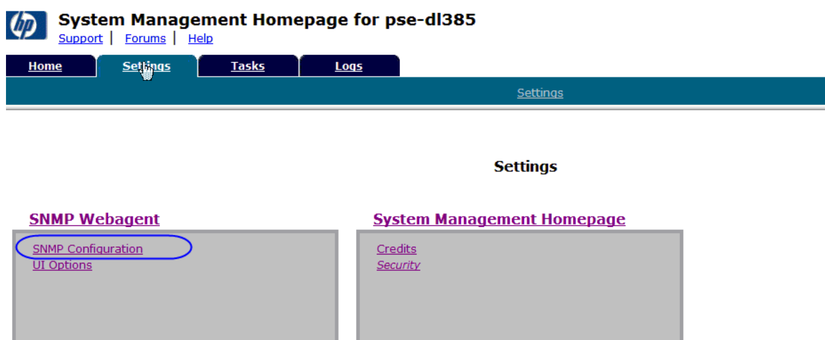
5.1.1 VMware ESX SNMP 設定

您可以在文字編輯器中存取 `snmpd.conf` 檔案，為來自受管理系統的 SNMP 通訊新增適用於 CMS 的 IP 位址，或者可以使用 System Management Homepage 來設定 SNMP。您需要針對每個 VMware ESX 受管理系統執行此動作。

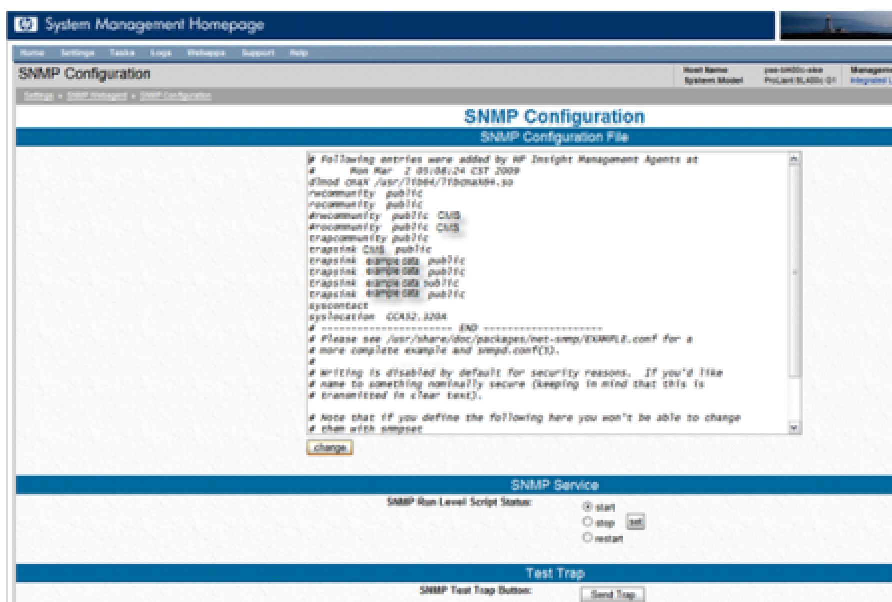
1. 使用 Web 瀏覽器存取受管理系統上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管理系統的 root 使用者名稱和密碼進行登入。



3. 按一下 **Settings** 標籤。



4. 按一下 **SNMP Configuration** 連結。
5. 在 **SNMP Configuration File** 中，新增 `trapsink` 指令，以包含 CMS 的 IP 位址 (例如，`trapsink 1.2.3.4 public`)，然後按一下 **Change**。

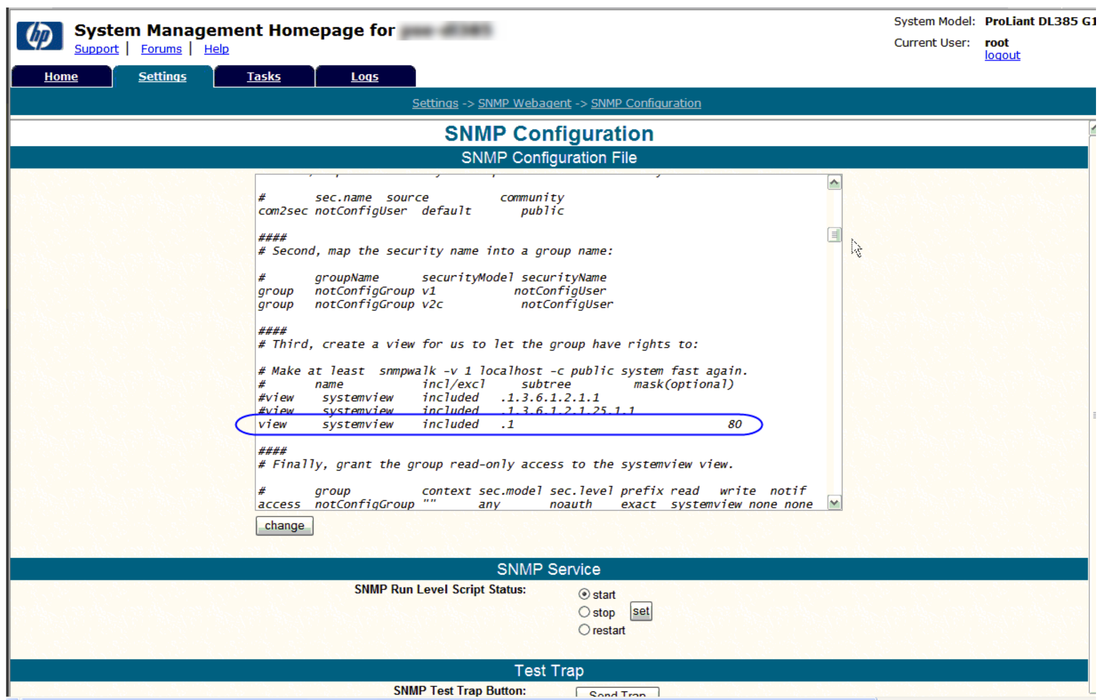




附註： 對於支援新增檢視陳述式之安全性的安裝，則應從預設值中進行下列調整。如果您沒有將 trapsink 項目指定爲 public，則必須爲這個受管理系統，以及 CMS 上任何其他透過 HP SIM 使用相同社群字串的系統，設定新的 SNMP 通訊協定。

6. 對於能夠收集所有關於此受管理系統之相關資訊的 CMS，您需要在 **SNMP Configuration File** 中向下捲動至 `view systemview included` 項目。將含有 `#` 字元的預設項目取消註解，然後新增此項目：

   `view systemview included .1 80`，接著按一下 **Change**。





附註： 如果您並未使用 SMH，也可以藉由在文字編輯器中編輯 snmpd.conf 檔案來執行此動作。

5.2 將 SNMP 測試 trap 傳送至 CMS

您可以遵循「VMware ESX SNMP 設定」中的說明，並且在 **Settings** 標籤上按一下 **Send Trap** 來使用 SMH 介面。但是，您也可以輸入下列指令，將測試 trap 發送至 CMS。

```
snmptrap -v1 -c public CMS IP Address.1.3.6.1.4.1.232 Linux Manage
System IP Address 6 11003 1234 .1.3.6.1.2.1.1.5.0 s test
.1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0 s "provide
your own identifiable identifier and time stamp"
```

如需有關檢閱測試指示或 trap 的詳細資訊，請參閱「檢閱受管理系統傳送的測試事件」。

6 Linux Integrity 受管理系統使用前提

6.1 從受管理系統中移除會導致衝突的舊版軟體

在設定受管理系統以搭配 CMS 上安裝的 Insight Remote Support Advanced A.05.40 版一起使用之前，您「必須移除所有」目前可能已安裝在受管理系統上的舊版 WEBES 或 HP ISEE Client。另外，也必須移除舊版 WCCProxy，但在 WEBES 解除安裝時通常也會自動將它一併解除安裝。

「唯有」當您在受管理系統上已安裝「任何」版本的 HP ISEE Client、WEBES 或 WCCProxy 時，才需要這些項目。如果您沒有安裝上述任何應用程式，請跳過這一節。

6.1.1 從 Linux 受管理系統中移除舊版應用程式

6.1.1.1 從 Linux 受管理系統中移除 HP ISEE

1. 關閉任何正在執行 ISEE Client 使用者介面的瀏覽器。
2. 以 root 身分 (系統管理權限) 登入受監視系統。
3. 切換至您安裝 HP ISEE 時所建立的目錄 (cd)。



附註： 此目錄名稱列在 /opt/hpservices/RemoteSupport/config/installDir 中

4. 若要從受監視系統中移除 HP ISEE 軟體，請執行下列指令：

```
bash uninstall.sh
```

6.1.1.2 從 Linux 受管理系統中移除 WEBES

使用互動式公用程式是移除整個 WEBES 套件最輕鬆的方法：

1. 執行下列指令來執行互動式工具：

```
/usr/sbin/webes_install_update utility
```

2. 選擇 *移除所有* WEBES 的選項
3. 依照任何出現的提示進行。

6.2 Integrity Linux 受管理系統需要 HP WBEM Providers



重要： 當您在中央管理伺服器 (CMS) 上設定 Insight Remote Support Advanced 時，「必須」在 HP SIM 介面中爲您的 Linux Integrity 受管理系統設定 WBEM 認證。《HP Insight Remote Support Advanced CMS 設定與使用手冊》的第二章詳細說明此程序。請將這些認證記下來，因爲您在稍後必須提供這些認證。

Integrity Linux 受管理系統上需要 HP WBEM Providers。HP 支援套件中提供 Integrity Linux HP WBEM Providers 及相關文件，而此套件是更大的 HP Integrity Essentials Foundation Pack for Linux 的一部分。HP SIM 也隨附於 Foundation Pack，但對 Insight Remote Support Advanced 而言*不是必要的或支援的*，因爲 Insight Remote Support Advanced 的 HP SIM/CMS 執行個體必須在 Windows ProLiant CMS 上執行。

您可以到 http://www.hp.com/go/integritylinuxessentials 取得最新版本的《HP Integrity Essentials Foundation Pack for Linux》軟體，也可以到 http://www.docs.hp.com/en/linux.html 取得最新版的文件；請在該網頁上搜尋 **HP Integrity Essentials Foundation Pack for Linux**。

6.3 將測試事件傳送至 CMS

若要從受管理系統傳送測試事件至 CMS，請從受管理系統的指令行輸入下列指令：

```
touch /tmp/SMX.test
```

這個指令會在 tmp 目錄中建立零長度的檔案，稱為 `SMX.test`。SMX 提供者會建立要傳送至 CMS 的指示，並移除您在上一步所建立的暫存檔。

7 Windows Integrity Server 受管理系統使用前提

7.1 概觀

請檢查《A.05.40 Insight Remote Support Advanced Release Notes》，在爲 Insight Remote Support Advanced 設定 Windows Integrity 系統之前，先確認該系統是受到支援的。接著，視需要完成下列各節：



附註： 針對 Windows 2008 支援，請套用下列項目：

- Service Pack One 需要 6.2 Insight Agents。
- Service Pack Two 或 Release Two 需要 6.5 Insight Agents。

WBEM 提供者可與系統中的 SNMP Agents 並存，只要其版本號碼相同即可。版本不符的 HP Insight Management WBEM 提供者與 HP Insight Management SNMP Agents 是不受支援的。

- 「從受管理系統中移除會導致衝突以及舊版的軟體」；如果您的受管理系統上已安裝任何舊版應用程式，請參閱本節
- 「正在執行 Windows 2003 的 Windows Integrity 受管理系統」；若要正確設定您的 Windows Integrity 受管理系統，本節是非常重要的。

7.2 從受管理系統中移除會導致衝突以及舊版的軟體

在設定受管理系統以搭配 CMS 上的 Insight Remote Support Advanced 一起使用之前，您「必須移除所有」目前可能已安裝在受管理系統上的舊版 WEBES 或 HP ISEE Client。另外，也必須移除舊版 WCCProxy，但在 WEBES 解除安裝時通常也會自動將它一併解除安裝。

「唯有」當您在 Windows Integrity 受管理系統上已安裝「任何」版本的 HP ISEE Client、WEBES 或 WCCProxy 時，才需要進行這些步驟。如果您沒有安裝上述任何應用程式，請跳過這一節。



重要： 如果在您計劃監視的環境中有一個以上的 HP NonStop 受管理系統，則這些受管理系統上必須要有 OSM。如需 NonStop 的設定指示，請參閱第 8 章「NonStop 受管理系統的安裝與設定」。如果您沒有 NonStop 系統，則不必參閱該章節。

7.2.1 移除 ISEE



小心： 如果您計劃使用 ISEE 移轉工具，將系統設定資料移轉至 CMS，則在您完成《HP Insight Remote Support Advanced CMS 設定與使用手冊》中定義的移轉步驟之前，請勿移除 ISEE。

1. 選取 **[開始]→[設定]→[控制台]→[新增/移除程式]**。
2. 從已安裝的程式清單中選取 **[HP Instant Support Enterprise Edition Client]**，然後按一下 **[變更/移除]**。

7.2.2 移除 WEBES

唯有當您已在受管理系統上安裝任何版本的 WEBES 時，才需執行這些步驟。如果您未安裝 WEBES，則可略過本節。

1. 使用具 `Administrator` 權限的帳戶登入 CMS。
2. 如果 WEBES 正在執行，請在 Command Prompt 中執行下列指令，完全關閉 WEBES (如果程序已經停止，則某些指令可能會傳回錯誤)：
   - `C:\> net stop desta_service`
   - `C:\> desta stop`
   - `C:\> net stop wccproxy`
   - `C:\> wccproxy kill`

3. 在 CMS 上，導覽至 [新增/移除程式]：

   開始 → 設定 → 控制台 → 新增/移除

4. 從已安裝程式清單中選取 **HP WEBES** 項目 (列出的舊版 WEBES 可能只會顯示 **WEBES**)。
5. 按一下 **[變更/移除]** 按鈕執行安裝精靈。
6. 在安裝精靈中，按一下**下一步**顯示修改與移除頁面。
7. 選擇**移除**選項。請不要選取**修改**選項。
8. 按一下**移除**，並按照提示繼續解除安裝。
9. 解除安裝程序完成後，請在「新增或移除程式」對話方塊中按 **F5** 鍵重新整理程式清單。

   如果列出 `WCCProxy` 程式，請選取該程式並按一下**移除**解除安裝。

   如果無法解除安裝 WCCProxy，請與 HP 客戶支援聯絡，以取得 WEBES 清除公用程式。

7.2.3 移除 OSEM

解除安裝將會完全移除 OSEM 目錄下的所有檔案。如有需要，您可以手動備援設定檔案，例如 `working.props`、`hosts.txt` 或 `communities.txt`。

1. 使用具有系統管理員權限的帳戶登入。
2. 將所有正在執行的工具全部關閉。
3. 在控制台中，連按兩下 **[新增/移除程式]**。
4. 在 **[新增/移除程式]** 對話方塊中，找出 OSEM 項目並按一下 **[移除]**，以執行安裝精靈。



小心： 在安裝精靈中，第一個 **Cancel** 是您徹底結束解除安裝常式的唯一機會。之後，即使有取消或結束選項可用，也不要再取消或停止解除安裝。

5. 遵循提示繼續解除安裝。

7.3 正在執行 Windows 2003 的 Windows Integrity 受管理系統

本節及其小節僅適用 Windows 2003 Integrity 受管理系統。如果 Windows 2003 不適用，請跳至「Windows 2008」一節。Event Log Monitoring Collector (ELMC) 負責在 Windows 2003 Integrity 受管理系統上監視遠端支援。WBEM 對於遠端資料收集是必要的。這兩者均會在下列各小節中進行處理。

7.3.1 滿足 ELMC 一般需求

受管理系統必須符合下列基本需要，您才能安裝 ELMC：

- 處理器架構：Integrity Server 上的 Itanium
- 作業系統：在 Integrity Server 上，Windows 2003 的所有支援版本
- 已在受管理伺服器上設定 TCP-IP
- 必要的權限與存取權：若要安裝、升級或解除安裝 WEBES 或 ELMC 元件，您必須以 Administrator 的身分登入，或以具備管理員權限的使用者登入。

7.3.2 在受管理系統上安裝 ELMC 軟體套件

將適當的 (IA64 或 x32/x64) ELMC Client 從 CMS 上的 RSSWM 下載資料夾複製到暫存目錄。按兩下以啓動安裝程序，該套件將在沒有任何使用者提示的情況下進行安裝並完成。您不需針對此軟體套件進行任何使用者設定輸入。

7.3.3 WBEM 和 Windows 2003 Integrity 受管理系統

若要讓您的 Windows 2003 Integrity 受管理系統能夠由 HP SIM 找到，並且能夠支援遠端資料收集，您就必須在受管理系統上安裝並完整設定 HP Integrity WBEM Providers for Windows Server 2003。因此，下列各節皆適用於 Windows 2003 和 Windows 2008 Integrity 受管理系統。

7.4 確認受管理系統上 WBEM 和 Agent Provider 的使用前提

若要讓您的 Windows Integrity 受管理系統能夠由 HP SIM 找到，並且能夠支援遠端資料收集，您就必須依照適當套件的《HP SmartSetup》產品文件中所指示，在受管理系統上安裝並完整設定 HP Integrity WBEM Providers for Windows Server。此情況適用於 Windows 2003 Integrity 受管理系統和 Windows 2008。Windows 2008 Integrity 受管理系統也會使用 WBEM 來進行事件提交/遠端監視。



附註： WBEM 提供者可與受管理系統系統上的 SNMP Agents 並存，只要其版本號碼相同即可。版本不符的 HP Insight Management WBEM 提供者與 HP Insight Management SNMP Agents 是不受支援的。

由 HP 製造出貨的 Windows Integrity Server 會在作業系統磁碟上預先載入 SmartSetup 安裝檔案。除此之外，您還可以使用 SmartSetup CD 或重新安裝媒體來安裝套件。您可以造訪 www.hp.com/go/integrity/windows，然後按一下 **Simplified management** 標題下方的 **Integrity Essentials for Windows** 連結，下載 SmartSetup Agents 或 Providers。

7.5 使用 WBEM Providers

對於要與 CMS 進行通訊的 WBEM Providers，您必須提供 WBEM 認證，如同《`HP Insight Remote Support Advanced CMS 設定與使用手冊`》的《`Configuring and Applying WBEM Credentials for Supported Managed Systems`》一節中所述。這些動作都必須在您正在完成 Insight Remote Support Advanced 設定時，於 CMS 上的 HP SIM 使用者介面內進行。

WBEM Providers 可以用來傳送 WBEM Indication 以確認連線，作法是存取 System Management Homepage，然後選取 **Settings** 標籤。接著，從 **Test Indication** 面板中，選取所顯示之 3 個嚴重性層級事件的其中一個，然後按一下 **Send**。

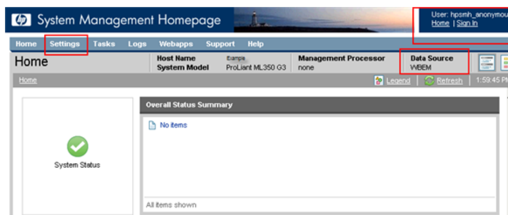
7.6 傳送 WBEM 測試指示

1. 使用 Web 瀏覽器存取受管理系統上的 System Management Homepage (SMH)：`http://ipaddress:2301`。
2. 使用受管理系統的系統管理員使用者名稱和密碼進行登入。

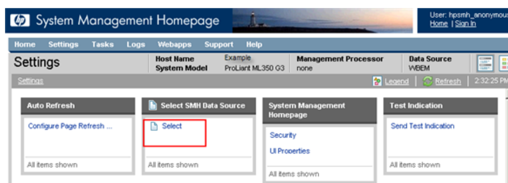


附註： 如果系統並未提示您登入，請檢查 SMH 介面的右上角，並按一下 **Sign In** 連結。如果沒有以系統管理員身分登入受管理系統，您將不會擁有所有的相關設定選項。

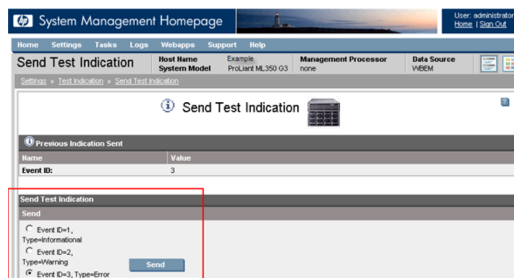
3. 按一下 **Settings** 選項。



4. 如果您選擇利用 Support Pack 來安裝 WBEM，將其設定為您的資料來源，請按一下 **Send Test Indication** 選項。



在 **Send Test Indication** 視窗中，選取事件 ID 類型 (任何可運作的類型)，然後按一下 **Send** 按鈕。



8 NonStop 受管理系統的安裝與設定



附註： 本章所含的資訊同時也存在於獨立文件《Insight Remote Support Advanced for NonStop》中，該文件位於 NonStop Technical Library 中 (網址為 http://docs.hp.com/en/NSSupport.html) 的 "NonStop Service Information" 底下。建議您查看該文件，以了解可能已更新的資訊。

8.1 概觀

HP Insight Remote Support Advanced 適用於 NonStop 系統，包括 HP Integrity NonStop BladeSystems、Integrity NonStop NS 系列的系統，以及 NonStop S 系列的系統。Insight Remote Support Advanced 是目前最新之適用於 NonStop 系統的遠端支援解決方案，可同時取代數據機及 HP Instant Support Enterprise Edition (ISEE) 遠端支援解決方案。

Insight Remote Support Advanced 是 HP Systems Insight Manager (SIM) 的外掛程式。此系統利用智慧型事件診斷，以及將硬體事件通知自動且安全提交給 HP 支援 (包括通知和狀態) 等方式來增強 HP SIM 的功能。

HP SIM 與 Insight Remote Support Advanced 都已安裝於 Windows 式中央管理伺服器 (CMS) 上 (請參閱「需求」)；最好是來自客戶資料中心內所有 NonStop 和其他 HP 平台的事件都可以傳送的中央伺服器。這可為整個資料中心的遠端支援提供單一的虛擬管理平台。

在 NonStop 系統上，OSM 會執行問題診斷並建立事件報告 (IR)。位於系統上的 OSM 軟體會將這些 IR 直接傳送至 Insight Remote Support Advanced (不需使用 OSM Notification Director)，接著將它們轉送給 HP 支援人員。

8.1.1 程序概觀

在 NonStop 環境中使用 Insight Remote Support Advanced 需要一些 HP SIM 與 Insight Remote Support Advanced 文件中所沒有提供的 NonStop 特定詳細資訊。本章為標準文件的補充說明，其中會概述步驟順序、提供那些文件的連結，以及說明開始使用 Insight Remote Support Advanced 時所需要執行之其他 NonStop 特定工作的時機與方法。在 NonStop 環境中開始使用 Insight Remote Support Advanced 的程序如下：

- 請確定已符合在 NonStop 環境中使用 Insight Remote Support Advanced 的所有「需求」。
- 執行「HP SIM 與 Insight Remote Support Advanced 的安裝與設定」。此程序包含一些要在程序中特定時機執行的「NonStop 特定的工作」 (包括停用 OSM Notification Director (ND))，如「Insight Remote Support Advanced 移轉案例」中所述。

8.2 需求

HP SIM 與 Insight Remote Support Advanced 都是安裝於稱為中央管理伺服器 (CMS) 的 Windows PC 上。雖然 HP 支援使用合格的 NonStop System Console (NSC) 做為 CMS，但是 HP 還是建議將 NSC 和 CMS 設定為兩台不同的伺服器。對於要設定做為 CMS 的 NSC，其必須執行 Windows 2003 Server，並配備至少 4 GB 的記憶體。目前只有執行 Windows Server 2003 之 CMS 上的 NonStop 系統才支援 Insight Remote Support Advanced。如需建議與替代設定圖表的範例，請參閱「主控台設定範例」。

表 8-1 NonStop 系統軟體需求：

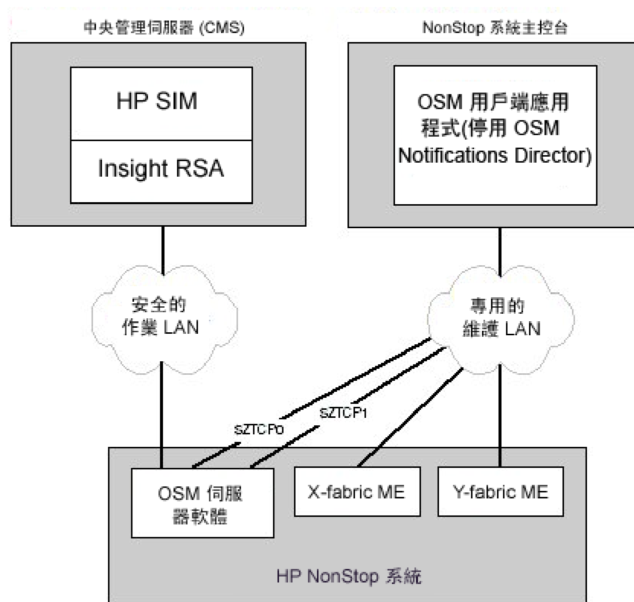
產品	最低版本
OSM (Nonstop 系統型軟體)	如果是 HP Integrity NonStop BladeSystems 或 Integrity NonStop NS 系列系統：T0682 ABU 或以上版本。 如果是 NonStop S 系列系統：T0682 ABY 或以上版本。
RVU	J06.03 或以上版本、H06.03 或以上版本、G06.10 或以上版本。

表 8-2 CMS 軟體需求：

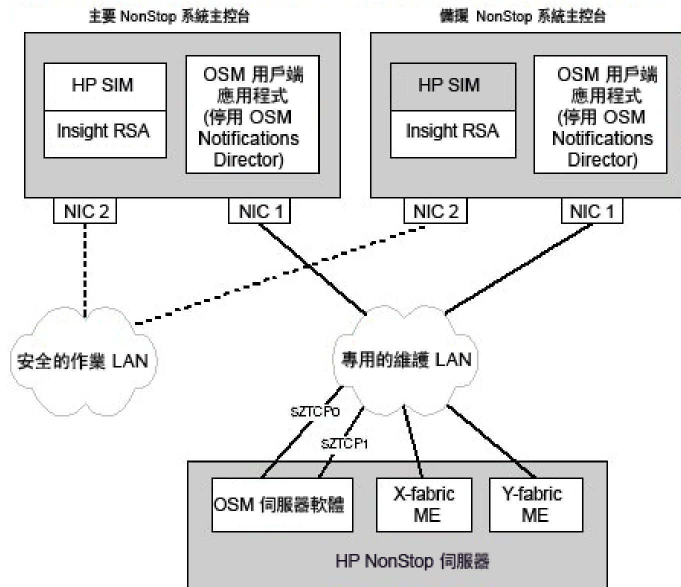
產品	最低版本	注意
HP SIM	5.3 (含 HotFix) 或以上版本	HP SIM 包括 Remote Support Software Manager (RSSWM)，其會在初始期間，安裝 Insight Remote Support Advanced 和必要的元件套件。
Insight Remote Support Advanced	A.05.20 或以上版本	已透過 RSSWM 下載並安裝。
WEBES	如果是 G 系列：5.6 或以上版本 如果是 H/J 系列：5.5 Patch 1 或以上版本*	Insight Remote Support Advanced 的元件，已透過 RSSWM 進行安裝。
	* 如果已經安裝，則也支援含 NonStop Support Patch 的 WEBES 5.5。如果您在含 NonStop Support Patch 且早於 5.5 的版本上安裝 WEBES 5.5 Patch 1，則會覆寫現有的 WEBM.jar 檔案。若無必要，還是建議您針對 H/J 系列使用 WEBES 5.6，請參閱「已知問題」，以取得升級到 5.6 版的優點。	
Remote Support 合格系統清單	A.05.20.24 或以上版本	Insight Remote Support Advanced 的元件，已透過 RSSWM 進行安裝。

8.2.1 主控台設定範例

第一個範例 (下圖所示) 顯示從 CMS (而非其中一個 NonStop 系統主控台) 執行 Insight Remote Support Advanced 的建議設定。儘管可能會有其他的 CMS 或 NSC 裝置 (圖表只展示其中一個)，此處的重點是 Insight Remote Support Advanced 並未在 NSC 上執行。



下圖所示的範例顯示用來從主要和備援 NonStop 系統主控台安裝和執行 Insight Remote Support Advanced 之建議設定的替代方法。



* 目前，HP SIM 中只支援監視 NonStop S 系列系統，而兩個主控台上的 Insight RSA 不會將重覆的事件傳送給 HP 支援中心。

8.3 HP SIM 與 Insight Remote Support Advanced 的安裝與設定

本節包含安裝和設定 HP SIM 與 Insight Remote Support Advanced 之 HP SIM 和 Insight Remote Support Advanced 文件的指標，以及要在安裝和設定程序期間之特殊時機執行的「NonStop 特定的工作」清單。請務必在安裝和設定 HP SIM 和 Insight Remote Support Advanced 時參閱「NonStop 特定的工作」一節，以便於適當時機執行這些額外的工作。

請遵循下列標題中，適用於您正在安裝之版本的手冊中所提供的指南來安裝 HP SIM 與 Insight Remote Support Advanced，網址為 http://docs.hp.com/en/netsys.html：

- HP Systems Insight Manager
- Insight Remote Support
- 遠端支援套件

8.3.1 NonStop 特定的工作

1. 安裝 HP SIM 5.3 之後，請下載並安裝適用於 HP SIM 5.3 - MS Windows 的 HotFix 更新套件 (含 SP1 的 HP SIM 5.3 也需要此更新套件)。您可以從下列網址取得此套件：http://h18013.www1.hp.com/products/servers/management/hpsim/dl_windows.html。



附註： 安裝套件時，其將會停止 HP SIM 服務、新增修補程式，然後重新啟動 HP SIM。當系統在 HP SIM 中探索您的 NonStop 系統，請等待，直到此程序提出要求為止。

2. WEBES `DESTA.REG` 檔案中有兩個設定必須要適當地設定，才能確保 NonStop 相容性。從 CMS 上的 DOS 提示字元中執行下列指令，以指定 `wbem.useip` 和 `wbem.destname` 參數所需的值：

   - `desta dri set wbem.useip t`
   - `desta dri set wbem.destname`

   接著，執行下列指令，讓 DESTA.REG 檔案的變更生效：

   - `net stop desta_service`
   - `net start desta_service`

3. 如果其不會用來監視該 CMS 上的任何 NonStop 系統，請停用 CMS 上的 OSM Notification Director (ND)，–或者–將 NonStop 系統設定為「非撥出點」，如「Insight Remote Support Advanced 移轉案例」中所述。
4. 在每個要監視的 NonStop 系統上設定 OSM – 必須在您的 OSMCONF 檔案中設定各種不同設定；這些設定會根據您的硬體平台和 LAN 設定而有所不同。

   停用 OSM ND 之後，請針對每個要受到 Insight Remote Support Advanced 監視的 NonStop 系統，在您的 OSMCONF 檔案中新增適當的旗標 (根據 NonStop 系統的類型而定)，以及啓用撥出至 Insight Remote Support Advanced/WEBES 的功能。

   - 如果是 NonStop BladeSystems，請新增：

     ```
     IR_Alert=YES
     ```

     ```
     Schema#NSK_DialoutConfiguration#Method#IrCalloutPathTest#OSMDisplayable
     = {"OSM_SC"}
     ```

     (Schema 參數必須在同一行，如此便不需承擔遭到所使用之編輯方法截斷行的風險)。

     ```
     EnableNDData=OFF
     ```

   - 如果是 NonStop NS 系列系統，請新增：

     ```
     IR_Alert=YES
     ```

     ```
     Schema#NSK_DialoutConfiguration#Method#IrCalloutPathTest#OSMDisplayable
     = {"OSM_SC"}
     ```

     (Schema 參數必須在同一行，如此便不需承擔遭到所使用之編輯方法截斷行的風險)。

     ```
     EnableNDData=OFF
     UseSSL=ON
     ```

   - 如果是 NonStop S 系列系統，請新增：

     ```
     IR_Alert=YES
     UseSSL=ON
     ```

   如果用於 Insight Remote Support Advanced 的 CMS 位於專用的維護 LAN 之外，則您必須在 OSMCONF 中，為 OSM 指定 stack 參數，如下所述：

   ```
   stack = <TCPIP 程序名稱>
   ```

   例如：

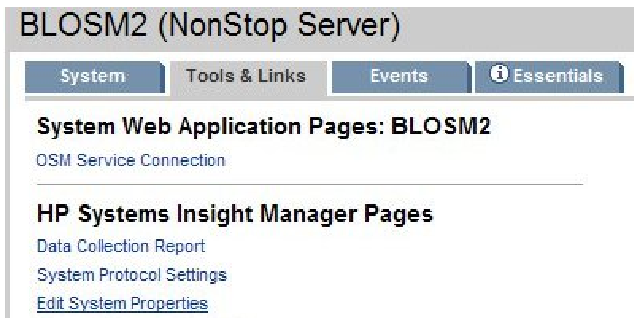
   ```
   stack = $ZTC00 stack = $ZTC01
   ```



附註： 編輯 OSMCONF 檔案之後，您必須重新啓動下列 OSM 伺服器程序 (如果是在 NonStop 系統上執行)，讓變更生效：

- $ZZKRN.#OSM-CIMOM
- $ZZKRN.#OSM-APPSRVR
- $ZZKRN.#OSM-OEV

5. 使用系統探索方法 (如適用於所使用之版本的 HP SIM 線上說明中所述)，來探索 HP SIM 中的每個 NonStop 系統 (不是 CMS)。探索過每個系統之後，可透過 HP SIM 中的 **Edit System Properties** 頁面來輸入下列 NonStop 授權值，以針對 Insight Remote Support Advanced 加以啓用。您可以在每個 NonStop 系統首頁上的 **Tools & Links** 標籤中存取該頁面 (如下圖所示)：



- 在 System Information > Identification 下方：於 Product number 欄位中輸入 **`NonStop`**。

System Information

Identification

Preferred system name: blosm3 Restore default name

☑ Prevent the Discovery process from changing this system name

Serial number: 551025

Product number: NonStop

- 在 Contract and Warranty Information > Entitlement Information 下方：
  - — System Country code：從下拉式功能表中選取適當的國家/地區：
  - — Entitlement type：輸入 **`System Handle`**
  - — Entitlement ID：輸入 **`NSKSUPPORT`**

Contract and Warranty Information

Entitlement Information

Customer-Entered serial number:

Customer-Entered product number:

System Country code: United States

Entitlement type: System Handle

Entitlement ID: NSKSUPPORT

按一下 **OK** 以儲存變更。

6. 對每個要受到 Insight Remote Support Advanced 監視的 NonStop 系統重複執行步驟 3-5。
7. 完成時，每個 NonStop 系統應該都會受到 Insight Remote Support Advanced 的監視。您可以使用 **Test Incident Report Delivery Paths** 動作 (位於 OSM Service Connection 中的 System 物件下方)，在每個系統上測試此功能。此動作會觸發定期事件報告。如果系統已受到 Insight Remote Support Advanced 監視，HP SIM 會在 Event 標籤上顯示事件，指出已報告 NonStop 系統事件。從 OSM 事件和警示的觀點：
   - 如果是 NonStop BladeSystems 和 NS 系列系統，一定會產生 OSM 事件 1103，表示 “Incident report delivery path not configured”，即使已成功傳遞 IR 也一樣。您可以忽略此事件 (如需詳細資訊，請參閱「已知問題」)。
   - 如果是 NonStop S 系列系統，OSM 會發出下列其中一個事件，以指出 IR 傳遞的嘗試成功或失敗：
     - — 事件 1102 (An Incident Report has been dialed out to the Support Center) – 會在至少一個路徑上成功進行 IR 傳遞時產生。如果第二個路徑失敗，即會在 System 物件上產生警示，其中會提供傳遞失敗之路徑的詳細資訊。
     - — 事件 1103 (An Incident Report has failed to be delivered) – 會在這兩個路徑上的 IR 傳遞都失敗時產生。系統會在 System 物件上產生警示，其中會提供傳遞失敗之路徑的詳細資訊。



附註： 如果是 NonStop S 系列系統 (在此時)，您可以基於容錯的目的，在一個以上的 CMS 上安裝和使用 Insight Remote Support Advanced。若要使用此設定，請在其他的 CMS 上重複執行步驟 1-7。

如果您在一個以上會管理 NonStop BladeSystems 或 NS 系列之系統的 CMS 上安裝和設定 Insight Remote Support Advanced，請確定只會在一個 CMS 上的 HP SIM 中執行這些系統的探索，以避免重複撥出。

8.4 Insight Remote Support Advanced 移轉案例

本節說明從使用 OSM Notification Director 移轉到 Insight Remote Support Advanced 的四個案例。當導向上述四個案例時，在「NonStop 特定的工作」的步驟 3 中，請遵循符合您現有主控台環境與設定之案例下方所列的步驟。



附註： 必須要設定 Insight Remote Support Advanced 或 OSM Notification Director (但不能同時設定) 來監視 NonStop 系統。HP 不支援已設定為同時支援 Insight Remote Support Advanced 和 OSM Notification Director 的 NonStop 系統。

此時，NonStop NS 系列系統和 NonStop BladeSystems 一次只能在一個 CMS 上受到 Insight Remote Support Advanced 監視 (請參閱「已知問題」)。

8.4.1 案例 1：使用 OSM ND，只監視單一 NSC 的一個 Nonstop 系統

1. 依序選取 **[開始]→[控制台]→[系統管理工具]→[服務]→`service_name`**，來停用下列服務。請確定不僅會停止服務，而且會將其 [啓動類型] 變更為 **[已停用]**。
   - 遠端 Proxy 服務
   - OSM Notification Director Monitor
2. 將下列可執行檔重新命名 (位於 `C:\OSM\bin` 中)，以防止他們意外啓動。例如，在 “`.exe`” 之後加上 “`.txt`” 副檔名，使其無法再執行。
   - `NDMonSvr.exe`
   - `OsmNd32.exe`
3. (選擇的) 若要從主控台移除 OSM Notification Director 和 Remote Proxy Service Start Menu 捷徑，請從 `C:\Documents and Settings\All Users\Start Menu\Programs\HP OSM` 中刪除下列資料夾：
   - `OSM Notification Director`
   - `Remote Proxy`
4. 返回「NonStop 特定的工作」的步驟 4，以完成啓用 Insight Remote Support Advanced 的程序。

8.4.2 案例 2：使用 OSM ND，只監視來自兩個 NSC (主要和備援 NSC) 的其中一個 Nonstop 系統

1. 遵循案例 1 下的步驟 1–3，以停用並移除主要 NSC 上的 OSM ND。
2. 遵循案例 1 下方的步驟 1–3，以停用並移除備援 NSC 上的 OSM ND。
3. 返回「NonStop 特定的工作」的步驟 4，以完成啓用 Insight Remote Support Advanced 的程序。

8.4.3 案例 3：使用 OSM ND，監視來自單一 NSC 的多個 Nonstop 系統

一次選取一個 Nonstop 系統，以執行這些 Insight Remote Support Advanced 移轉步驟：

1. 啓動 OSM ND，並從 Systems 功能表中選取 **Configure \system_name**。
2. 登入。在 Preferences 標籤上的 Dial-out Definition 下方，選取 **Not a Dial-out Point**，然後按一下 **OK**

3. 返回「NonStop 特定的工作」的步驟 4，以完成在每個 NonStop 系統上啓用 Insight Remote Support Advanced 的程序。但是，請確定會返回此「案例 3」程序，並針對每個要移轉至 Insight Remote Support Advanced 的 NonStop 系統重複執行步驟 1-3。
4. 如果所有的 NonStop 系統都已移轉至 Insight Remote Support Advanced，請遵循案例 1下的步驟 1–3 來停用 OSM ND。但是，如果有些 NonStop 系統將繼續受到 ND 監視，則請勿執行這些步驟來停用並移除 ND。

8.4.4 案例 4：使用 OSM ND，監視來自兩個 NSC (主要和備援 NSC) 的多個 NonStop 系統

一次選取一個 Nonstop 系統，以執行這些 Insight Remote Support Advanced 移轉步驟。開始使用備援 NSC：

1. 啓動 OSM ND，並從 Systems 功能表中選取 **Configure \system_name**。
2. 登入。在 Preferences 標籤上的 Dial-out Definition 下方，選取 **Not a Dial-out Point**，然後按一下 **OK**
3. 移動至主要 NSC，並重複執行上述的步驟 1 和 2 (在案例 4 下)。
4. 返回「NonStop 特定的工作」的步驟 4，以完成在每個 NonStop 系統上啓用 Insight Remote Support Advanced 的程序。但是，請確定會返回此「案例 4」程序，並針對每個要移轉至 Insight Remote Support Advanced 的 NonStop 系統重複執行步驟 1-4。
5. 在備援 NSC 上：如果所有受到此主控台監視的 NonStop 系統都已移轉至 Insight Remote Support Advanced，請遵循案例 1下的步驟 1-3 來停用 OSM ND。但是，如果有些 NonStop 系統將繼續受到 ND 監視，則請勿執行這些步驟來停用並移除 ND。
6. 在主要 NSC 上：如果所有受到此主控台監視的 NonStop 系統都已移轉至 Insight Remote Support Advanced，請遵循案例 1下的步驟 1-3 來停用 OSM ND。但是，如果有些 NonStop 系統將繼續受到 ND 監視，則請勿執行這些步驟來停用並移除 ND。

8.5 已知問題

這些問題僅適用於 NonStop NS 系列系統與 NonStop BladeSystems，不適用於 NonStop S 系列系統：

- Insight Remote Support Advanced 目前無法在這些系統的容錯 CMS 設定中使用。如果您在一個以上會管理 NonStop BladeSystems 或 NS 系列之系統的 CMS 上安裝和設定 Insight Remote Support Advanced，請確定只會在一個 CMS 上的 HP SIM 中執行這些系統的探索，以避免重複撥出。
- 系統一定會建立下列 OSM 子系統事件，即使事件報告已成功傳遞至 CMS 也一樣。您可以忽略此事件，因爲它代表 IR 路徑的容錯本質，此爲目前版次中的一個已知限制：

  ```
  OSM 子系統事件 1103。An Incident Report has failed to be delivered.
  原因：事件報告傳遞路徑尚未設定。
  ```

  若要查看事件報告的傳遞狀態，請查看 HP SIM 內的 Events 標籤。



附註： 升級至 WEBES 5.6 會提供其他資訊，以指出 IR 傳遞嘗試是成功或失敗。使用 WEBES 5.6，不論 IR 是否已傳遞，您仍會取得該事件 (如上所述)；但是，您也可以取得下列其中一個事件，指出 IR 傳遞嘗試是成功或失敗：

```
1102. An Incident Report has been dialed out to the Support Center for IR id#.
```

或

```
1103. An Incident Report has failed to be delivered.IR id#
```

(在此案例中，事件 1103 可能會列出 "Incident report delivery path not configured" 以外的原因，或者完全不會列出任何原因。)

如果您取得事件 1102 以及最初的 1103 事件，則表示 IR 已成功傳遞。如果您不是取得事件 1102，而是取得第二個 1103 事件，則表示 IR 並未成功傳遞。

8.6 撤回

如果您希望撤回 Insight Remote Support Advanced 而改回使用 OSM Notification Director，請視需要執行下列工作 (根據您在移轉至 Insight Remote Support Advanced 期間是否刪除或只停用 ND 而定)：

- 如果您完全不會再使用 HP SIM，請停止 HP Systems Insight Manager (**[開始]**→**[控制台]**→**[系統管理工具]**→**[服務]**)，或者，如果您將繼續使用 HP SIM 來監視其他系統，則只需從 HP SIM 刪除個別的 NonStop 系統。
- 移除在 OSMCONF 設定工作期間插入的 OSMCONF 旗標，然後重新啓動 OSM 伺服器程序，讓這些變更生效。
- 視需要復原所執行的步驟，以便在 Insight Remote Support Advanced 移轉的案例 1期間，停用 OSM Notification Director 和 Remote Proxy Service。如果您已刪除 OSM Notification Director 和 Remote Proxy Service Start Menu 捷徑，則需要重新安裝這些產品。若未刪除，則只需將檔案重新命名爲其原始名稱，並重新啓動服務即可。
- 如果已從 OSM Notification Director 中刪除個別系統 (如同案例 3和案例 4中所要求)，請在 OSM Notification Director 內重新設定每個 NonStop 系統。

9 Insight Remote Support 的 HP-UX 受管理系統需求

9.1 概觀

本文說明 HP-UX 受管理系統要符合 Insight Remote Support Advanced 資格所必須具有的狀態。在嘗試將 HP Insight Remote Support 加入至您的 HP-UX 受管理系統之前，請仔細並完整閱讀本文。

1. 驗證硬體支援

   由於產品支援可能有所變更，已超出主要軟體版本的範圍，請務必查閱《A.05.40 Insight Remote Support Advanced Release Notes》，以確認您的硬體目前有受到支援。

2. 移除發生衝突的軟體

   如果 ISEE 或 Insight Remote Support 完全不支援此 HP-UX 受管理系統，請略過此步驟。如果正在將現有的 Instant Support Enterprise Edition (ISEE) Client 移轉至 Insight Remote Support，您「必須移除」下列軟體應用程式：

   - 「任何」舊版的 WEBES
   - 「任何」版本的 HP Instant Support Enterprise Edition (ISEE)

   如果 Insight Remote Support (先前稱為 RSP) A.05.05 版支援此 HP-UX 受管理系統，則您必須移除 A.05.05 ACC 元件 (如果已安裝的話)。

   如需移除這些元件 (ISEE、WEBES 或 A.05.05 ACC) 的指示和注意事項，請參閱「移除衝突的軟體」。

3. 確認符合作業系統、軟體及修補程式需求。

   如需特定 HP-UX 作業系統需求的詳細資訊，請參閱「符合 HP-UX 作業系統、軟體及修補程式需求」。

4. 建立通訊和設定通訊協定

   在所有支援的 HP-UX 版本上，HP Insight Remote Support 通訊都需要系統錯誤管理 (SFM)。SFM 有許多修補程式使用前提，「符合 HP-UX 作業系統、軟體及修補程式需求」中會詳細說明。如果您的系統已符合該節中所指出的最低需求，則不需要移除或重新安裝那些元件。如果您的系統不符合最低需求，請依照「深入了解 WBEM 和 SFM 及 Insight Remote Support」中的指示進行升級。



附註： 您可能已熟悉不同 SFM 產品中提供的各種 SFM 提供者。Insight Remote Support 只需要標準 SFM 套件中的提供者，如「符合 HP-UX 作業系統、軟體及修補程式需求」中所指定。

5. 安裝和設定進階設定收集器

   進階設定收集器 (ACC) 元件是用於產生主動服務設定集合並傳送給 HP。如果您不在關鍵性支援合約所涵蓋的範圍內，則不需要安裝或設定 ACC 元件。如果您在關鍵性支援所涵蓋的範圍內，請依照「移除 B.05.05 進階設定收集器 (ACC) 軟體套件」中的指示進行。

6. 完成 CMS 設定

   本簡短文件只說明 HP-UX 受管理系統的需求。當您的受管理系統已確實符合所有必要需求之後，就必須設定 CMS 來與受管理系統進行通訊。《HP Insight Remote Support Advanced CMS 設定與使用手冊》中會說明這些程序。



重要： 當您在中央管理伺服器 (CMS) 上設定 Insight Remote Support Advanced 時，「必須」在 HP SIM 介面中為您的 HP-UX 受管理系統設定 WBEM 認證。《HP Insight Remote Support Advanced CMS 設定與使用手冊》的第二章詳細說明此程序。請將這些認證記下來，因為您在稍後必須提供這些認證。

9.2 移除衝突的軟體

「唯有」當您在 HP-UX 受管理系統上已安裝「任何」版本的 HP ISEE Client 或 WEBES 時，才需要進行這些步驟。



小心： 如果您計劃使用 ISEE 移轉工具，將系統設定資料移轉至 CMS，則在您完成《HP Insight Remote Support Advanced CMS 設定與使用手冊》中定義的移轉步驟之前，請勿移除 ISEE。

9.2.1 從 HP-UX 受管理系統中移除 HP ISEE

「唯有」當您在受管理系統上已安裝 HP Instant Support Enterprise Edition 時，才需要進行這些步驟。如果您沒有在受管理系統上安裝 ISEE，可以跳過這一節。



重要： Instant Support Enterprise Edition (ISEE) A.03.95 及舊版與 Insight Remote Support Advanced「不是相同的應用程式」，請不要安裝在任何受管理系統上。

若要移除 ISEE，請完成下列步驟：

1. 以 `root` 身分 (系統管理權限) 登入受監視系統。
2. 在每一個受管理系統上執行下列指令：

   ```
   /usr/sbin/swremove ISEEPlatform
   ```

   如果 `swremove` 程序執行成功，則會顯示已移除軟體的確認訊息。請檢查記錄檔，確認沒有任何錯誤。

   如果 `swremove` 程序未順序完成，請參閱產生的記錄檔。其中可能指出導致失敗的 ISEE 平台相依性。VAEH、Availability Measure 或 CCMon 等元件都是選擇的商務支援軟體元件，但必須先移除這些元件，ISEE 平台才能完成解除安裝。

   請針對記錄檔中列出的每一個商務支援軟體元件來執行 `swremove`。如需這些元件的相關資訊，請參閱《HP Instant Support Enterprise Edition Client Installation and Upgrade Guide》A.03.95.500 中的 Business Support Software 元件章節，網址為：http://sstwww.fc.hp.com/ISEE/client/A.03.95.500client.pdf

9.2.2 從 HP-UX 受管理系統中移除 WEBES

執行互動式 `webes_install_update utility`，選擇移除所有 WEBES 的選項，並依照任何出現的提示進行。

9.2.3 移除 B.05.05 進階設定收集器 (ACC) 軟體套件

在安裝 A.05.40 版 ACC 軟體套件之前移除 B.05.05 版。若要移除此套件，請在每一個 HP-UX 受管理系統上執行下列指令：

```
swremove RS-ACC
```

在 CMS 上，使用 HP SIM 來探索您的 HP-UX 受管理系統，且在 CMS 上安裝 WEBES 之前，依照第 4 章所述來設定系統資訊。根據您的 HP SIM 設定而定，系統可能會自動執行探索。

9.3 符合 HP-UX 作業系統、軟體及修補程式需求

請參閱下表，確認您的 HP-UX 受管理系統已正確設定成符合 Insight Remote Support 的需求。

9.3.1 HP-UX 11.11 的軟體和修補程式需求



重要： 雖然並非 HP-UX 11.11 所需 ，但還是強力建議使用 `GOLDBASE11i - B.11.11.0612.459 Base Patches for HP-UX (December 2006)`。安裝 GOLDBASE11i 可滿足所有系統修補程式需求，也能為客戶提供穩定的支援環境。下表指出最低的必要修補程式 (未安裝 GOLDBASE11i 時需要)。



附註： 下表的注意事項

- Operating Environment (OE) 媒體中包含 WBEM Services、Online Diagnostics、SysMgmtWeb 及 HP SIM，在 SFM 安裝期間可選擇安裝。Insight Remote Support 不支援 HP-UX 上的 HP SIM。
- 列出的軟體版本是最低的支援需求。除非另外註明，否則較新的版本都可相容。
- SysMgmtWeb 中隨附的 System Management Homepage (SMH) 為選擇的項目。但是，如果沒有安裝，則無法存取 Event Viewer (EvWEB) 使用者介面。
- 如果存在舊版的 SFM (A.01.00.01 或 A.03.00.xx)，則必須先解除安裝，才能安裝 SFM A.04.00.04 版。
- 此表格中的項目是根據任何項目在遺漏而需要升級或安裝時應該遵循的安裝順序列出。

表 9-1 HP-UX 11.11 的必要軟體元件

需要的軟體	需要的版本
`HP-UX 作業環境`	11i V1
如何下載或取得軟體： http://h20338.www2.hp.com/hpux11i/cache/324916-0-0-0-121.html	
作業系統修補程式需求	支援任何 11.11 OE，但 2003 年 6 月以前的任何 11.11 OE 也都必須安裝修補套件 B.11.11.0306.1。
如何下載 HP-UX 的修補程式： 前往 http://itrc.hp.com/service/patch/hpuxPatchBundlePage.do?bundleId=BUNDLE11i:B.11.11.0306.1	
`OpenSSL`	`A.00.09.07i.012 產品組合 (2006 年 12 月) 或以上版本`
如何下載或取得軟體： • 自 2006 年 12 月起透過應用程式軟體媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I	
`WBEMServices` (WBEM Services 核心產品)	`A.02.05 產品組合 (2006 年 12 月)`
如何下載或取得軟體： • 自 2006 年 12 月起透過應用程式軟體媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs	
`Online Diagnostics`	`B.11.11.18.05 產品組合 (2006 年 12 月)`

表 9-1 HP-UX 11.11 的必要軟體元件 (繼續)

需要的軟體	需要的版本
如何下載或取得軟體： • 透過 HWE0612 媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE	
System Management Web (事件監視的建議元件，設定收集的必要元件)	A2.2.5 產品組合 (2006 年 12 月)
System Management Web 為選擇元件，但可讓您充分利用「系統故障管理」的 EVWEB GUI 元件，以檢視 SFM 在主機上所處理的事件。 如果系統上只有 SysMgmtHomepage 2.2.6.2 版，則還必須安裝下列修補程式： 如果是 HP-UX 11iv1 (11.11) OE，則必須安裝修補程式 PHSS_36869 您可以從位於下列 URL 的 IT 資源中心取得修補程式： ftp://ftp.itrc.hp.com/hp-ux_patches/s700_800/11.X/'patch number' 這是「shar 壓縮檔」，必須以指令檔的形式執行來解壓縮 (“sh PHSS_36869)。請務必檢閱隨附之文字檔中的修補程式安裝指示 (PHSS_36869.text)	
如何下載或取得軟體： • 自 2007 年 12 月起透過應用程式軟體媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb	
hpuxwsApache	A.2.0.49
只有對進階設定收集器元件而言 (做為遠端支援的 HP Remote Support Configuration Collection 項目的代理程式)，hpuxwsApache 才是必要元件。對遠端支援監視而言不是必要元件。	
安裝 hpuxwsAPACHE 產品時，建議安裝整個 hpuxwsApache 組合。若為已下載的軟體庫，則不需要 hpuxTomcat 和 hpuxWebmin 組合。	
如何下載或取得軟體： • 透過 11.11 Jun04 OE/AR 或以上版本的媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=HPUXWSATW218	
系統故障管理 (SFM)	A.04.00.04 產品組合 (2006 年 12 月)
SFM 必須是從這份清單中安裝或升級的最後一個必要軟體元件。	
如何下載或取得軟體： • 透過 HWE0612 媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysFaultMgmt	

9.3.2 HP-UX 11.23 的軟體和修補程式需求



重要： 雖然並非 HP-UX 11.23 所需 ，但還是強力建議使用 `QPKBASE B.11.23.0712.070 Base Quality Pack Bundle for HP-UX 11i v2 (December 2007)`。

安裝 QPKBASE B.11.23.0712.070 可滿足所有系統修補程式需求，也能為客戶提供穩定的支援環境。下表指出最低的必要修補程式 (未安裝 QPKBASE B.11.23.0712.070 時需要)。

重要： 在 CMS 上，使用 HP SIM 來探索您的 HP-UX 受管理系統，並且在安裝 WEBES 之前，依照第 4 章所述來設定系統資訊。根據您的 HP SIM 設定而定，系統可能會自動執行探索。



附註： 下表的注意事項

- Operating Environment (OE) 媒體中包含 WBEM Services、Online Diagnostics、SysMgmtWeb 及 HP SIM，在 SFM 安裝期間可選擇安裝。Insight Remote Support 不支援 HP-UX 上的 HP SIM。
- 列出的軟體版本是最低的支援需求。除非另外註明，否則較新的版本都可相容。
- SysMgmtWeb 中隨附的 System Management Homepage (SMH) 為選擇的項目。但是，如果沒有安裝，則無法存取 Event Viewer (EvWEB) 使用者介面。
- 如果存在舊版的SFM (A.01.00.01 或 A.03.00.xx)，則必須先解除安裝，才能安裝SFM A.04.00.04 版。
- 此表格中的項目是根據任何項目在遺漏而需要升級或安裝時應該遵循的安裝順序列出。

附註： 對於 HP-UX 端點系統上的 ELMC 軟體沒有特定需求，因為在 HP-UX 系統上，WEBES 會直接與 CIM Object Manager (CIMOM) 進行通訊。另外也會移除 WCCProxy，但是在 WEBES 解除安裝時自動將它一併解除安裝。



重要： 在 CMS 上，使用 HP SIM 來探索您的 HP-UX 受管理系統，並且在安裝 WEBES 之前，依照第 4 章所述來設定系統資訊。根據您的 HP SIM 設定而定，系統可能會自動執行探索。

表 9-2 HP-UX 11.23 的必要軟體元件

需要的軟體	需要的版本
HP-UX 作業環境	• 2004 年 9 月 11i v2 OE (OE 最低版本) • 2005 年 5 月 11i V2 OE (vPars 有啓用 vPars 時)。
如何下載或取得軟體： http://h20338.www2.hp.com/hpux11i/cache/324923-0-0-0-121.html	
作業系統修補程式需求 **附註：** HP-UX 11i v2 的這六個額外修補程式「不是」Bundle11i 的一部分，必須另外安裝。	BUNDLE 11i 修補程式組合 B.11.23.0409.3 (2004 年 9 月)： • PHKL_36288 - 11.23 diag2 綜合驅動程式及 vPars 啓用 (用來取代 PHKL_32653)，需要重新開機 • PHKL_34795 - 11.23 IPMI 綜合驅動、修補程式，需要重新開機 • PHSS_37552 1.0 Aries 綜合修補程式 • PHSS_37947 1.0 連結器 + fdp 綜合修補程式 • PHSS_35055 - aC++ Runtime (IA：A.06.10，PA：A.03.71) • PHSS_36345 - 11.23 Integrity Unwind Library
如何下載或取得軟體： 前往 www.hp.com，選取 **Support and Drivers** 標籤。然後，按一下網頁右邊的 **Download patches for HP-UX, Open VMS, Tru64 and MPE** 按鈕。這時會連結至 ITRC，讓您搜尋適當的修補程式。	

表 9-2 HP-UX 11.23 的必要軟體元件 (繼續)

<table>
<tr><th>需要的軟體</th><th>需要的版本</th></tr>
<tr><td colspan="2"></td></tr>
<tr><td>OpenSSL</td><td>A.00.09.07i.012 產品組合 (2006 年 12 月) 或以上版本</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
• 自 2006 年 12 月起透過應用程式軟體媒體提供
• 或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Online Diagnostics</td><td>B.11.23.10.05 產品組合 (2007 年 12 月)</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
• 透過 HWE0706 媒體提供
• 或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>WBEMServices (WBEM Services 核心產品)</td><td>A.02.05.08 產品組合 (2007 年 12 月)</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
• 自 2007 年 12 月起透過應用程式軟體媒體提供
• 或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>System Management Web (事件監視的建議元件，設定收集的必要元件)</td><td>A.2.2.7 產品組合 (2007 年 12 月)</td></tr>
<tr><td colspan="2">建議安裝 System Management Web，以充分利用「系統故障管理」的 EVWEB GUI 元件，以檢視 SFM 在主機上所處理的事件。
如果系統上只有 SysMgmtHomepage 2.2.6.2 版，則還必須安裝下列修補程式：
如果是 HP-UX 11iv2 (11.23) OE，則必須安裝修補程式 PHSS_36870
您可以從位於下列 URL 的 IT 資源中心取得修補程式：
ftp://ftp.itrc.hp.com/hp-ux_patches/s700_800/11.X/'patch number'
這是「shar 壓縮檔」，必須以指令檔的形式執行來解壓縮 (“sh PHSS_36870)。請務必檢閱隨附之文字檔中的修補程式安裝指示 (PHSS_36870.text)</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
• 自 2007 年 9 月起透過應用程式軟體媒體提供
• 或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>hpuxwsApache</td><td>A.2.0.49</td></tr>
<tr><td colspan="2">只有對進階設定收集器元件而言 (做爲遠端支援的 HP Remote Support Configuration Collection 項目的代理程式)，hpuxwsApache 才是必要元件。對遠端支援監視而言不是必要元件。</td></tr>
<tr><td colspan="2">安裝 hpuxwsAPACHE 產品時，建議安裝整個 hpuxwsApache 組合。若爲已下載的軟體庫，則不需要 hpuxTomcat 和 hpuxWebmin 組合。</td></tr>
</table>

表 9-2 HP-UX 11.23 的必要軟體元件 (繼續)

需要的軟體	需要的版本
如何下載或取得軟體： • 透過 11.23 Sep04 OE/AR 或以上版本的媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=HPUXWSATW218	
HPUXBaseAux.SysMgmtBase 或 SysMgmtBASE.SysMgmtBase	A.2.0.49
只有對 Advanced Configuration Collector 元件而言 (做為遠端支援的 HP Remote Support Configuration Collection 項目的代理程式)，此元件才是必要元件。對遠端支援監視而言不是必要元件。	
從 HPUXBaseAux 組合中安裝產品 SysMgmtBase 時，不需要安裝整個組合。	
如何下載或取得軟體： • 11.23 Sep06 OE 或以上版本 (例如 HPUXBaseAux.SysMgmtBase)，或是 11.23 Sep06 AR 或以上版本 (例如 SysMgmtBASE.SysMgmtBase) • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=SysMgmtBASE	
系統故障管理 (SFM)	B.05.00.05 產品組合 (2007 年 12 月)
SFM 必須是從這份清單中安裝或升級的最後一個必要軟體元件。	
如何下載或取得軟體： • 透過 HWE0712 媒體提供 • 或者，前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysFaultMgmt	

9.3.3 HP-UX 11.31 的軟體和修補程式需求



附註： 下表的注意事項

- Operating Environment (OE) 媒體中包含 WBEM Services、Online Diagnostics、SysMgmtWeb 及 HP SIM，在 SFM 安裝期間可選擇安裝。Insight Remote Support 不支援 HP-UX 上的 HP SIM。
- 列出的軟體版本是最低的支援需求。除非另外註明，否則較新的版本都可相容。
- SysMgmtWeb 中隨附的 System Management Homepage (SMH) 為選擇的項目。但是，如果沒有安裝，則無法存取 Event Viewer (EvWEB) 使用者介面。
- 如果存在舊版的 SFM (A.01.00.01 或 A.03.00.xx)，則必須先解除安裝，才能安裝 SFM A.04.00.04 版。
- 此表格中的項目是根據任何項目在遺漏而需要升級或安裝時應該遵循的安裝順序列出。

表 9-3 HP-UX 11.31 的必要軟體元件

需要的軟體	需要的版本
HP-UX 作業環境	HP-UX 11i V3
如何下載或取得軟體： http://h20338.www2.hp.com/hpux11i/cache/458092-0-0-0-121.html	

表 9-3 HP-UX 11.31 的必要軟體元件 (繼續)

<table>
<tr><th>需要的軟體</th><th>需要的版本</th></tr>
<tr><td>作業系統修補程式需求</td><td>EVM-Event Mgr B.11.31
Baseboard Management Controller (BMC) 韌體 70.59 版或以上版本
Sys MgmtBase B.00.02.03</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
前往 www.hp.com，選取 Support and Drivers 標籤。然後，按一下網頁右邊的 Download patches for HP-UX, Open VMS, Tru64 and MPE 按鈕。這時會連結至 ITRC，讓您搜尋適當的修補程式。</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>OpenSSL</td><td>A.00.09.07e.013 或以上版本</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
自 2007 年 9 月起透過應用程式軟體媒體提供
或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>HP-UX 診斷和支援工具；包括 STM A.49.10 版或以上版本及 EMS A.04.20 版或以上版本</td><td>B.11.31.01.yy</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
透過 HP-UX 11i v3 - 2007 年 2 月媒體提供
或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>WBEMServices (WBEM Services 核心產品)</td><td>A.02.05 或以上版本</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
自 2007 年 9 月起透過應用程式軟體媒體提供
或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>System Management Web (建議，非必要)</td><td>A.2.2.4</td></tr>
<tr><td colspan="2">建議安裝 System Management Web，以充分利用「系統故障管理」的 EVWEB GUI 元件，以檢視 SFM 在主機上所處理的事件。
如果系統上只有 SysMgmtHomepage 2.2.6.2 版，則還必須安裝下列修補程式：
如果是 HP-UX 11iv3 (11.31) OE，則必須安裝修補程式 PHSS_36871
您可以從位於下列 URL 的 IT 資源中心取得修補程式：
ftp://ftp.itrc.hp.com/hp-ux_patches/s700_800/11.X/'patch number'
這是「shar 壓縮檔」，必須以指令檔的形式執行來解壓縮 (“sh PHSS_36871)。請務必檢閱隨附之文字檔中的修補程式安裝指示 (PHSS_36871.text)</td></tr>
<tr><td colspan="2">如何下載或取得軟體：
自 2007 年 9 月起透過應用程式軟體媒體提供
或者，前往下列 HP 軟體庫位置取得最新版本：
https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>系統故障管理</td><td>C.01.00.29.yy</td></tr>
</table>

表 9-3 HP-UX 11.31 的必要軟體元件 (繼續)

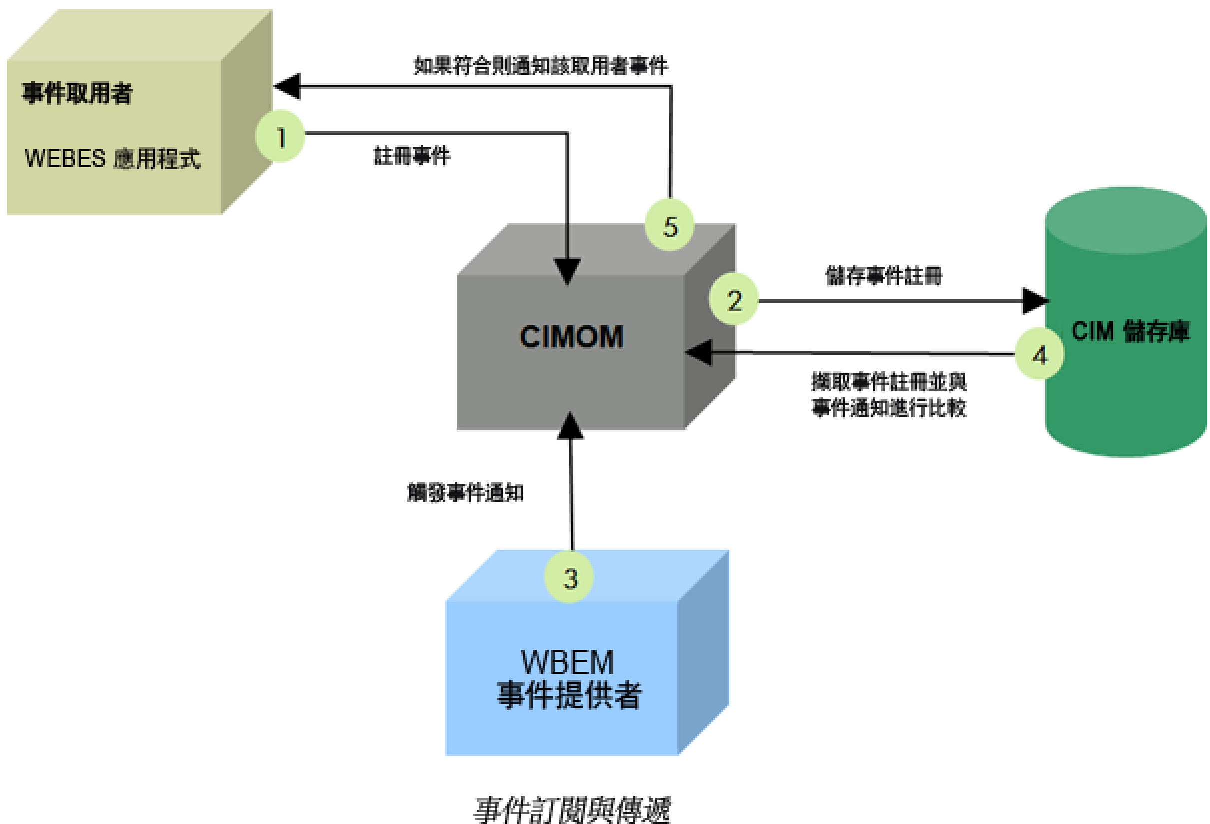
需要的軟體	需要的版本
SFM 必須是從這份清單中安裝或升級的最後一個必要軟體元件。	
如何下載或取得軟體： 前往下列 HP 軟體庫位置取得最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysFaultMgmt	

9.4 深入了解 WBEM 和 SFM 及 Insight Remote Support

Web-Based Enterprise Management (WBEM) 是將不同平台的管理資訊標準化的一套產業計劃。系統故障管理 (SysFaultMgmt 或 SFM) 是採用 WBEM 標準的 HP-UX 錯誤管理解決方案。系統故障管理與其他如 HP SIM、HP SMH 等容易管理的應用程式，和任何其他的 WBEM Client (例如 WEBES) 整合在一起。SFM 要求 HP-UX 必須安裝 `WBEM Services for HP-UX` 和其他軟體。

WBEM 中的事件稱爲指示。Client 系統 (例如 CMS) 必須先訂閱事件，才能向 Client 系統回報指示。事件訂閱可以讓受管理系統的 `Common Information Model Object Manager` (CIMOM) 知道 Client (CMS) 想要接收來自該受管理系統 (端點) 的指示。當 CIMOM 收到來自指示提供者的指示時，它會將指示傳送至先前已訂閱要接收這些指示的 Client。

CMS 上的 WEBES 會訂閱這些指示。完成訂閱後，指示發生時就會傳遞至 CMS 上的 WEBES。下圖提供事件 (指示) 訂閱和傳遞流程的簡單概觀。



事件訂閱與傳遞

如需 SFM 更詳細的資訊，請參閱《`OE/AR Depot Information for HP-UX WBEM Providers`》中關於這些提供者的概觀，網址爲 http://h10018.www1.hp.com/wwsolutions/misc/hpsim-helpfiles/OEARInformation.pdf。

9.5 確認「系統故障管理」可以正常運作

若要確認「系統故障管理」元件 (SFM) 可以在 HP-UX 受管理系統上正常運作，請執行下列動作：

1. 執行下列指令，檢查是否已安裝 `HP WBEM Services for HP-UX` 元件：

   `# swlist | grep -i WBEM`

   應該會傳回類似下列的輸出：

   ```
   # swlist | grep -i WBEM
     LVMProvider          R11.23.008      CIM/WBEM Provider for LVM
     ProviderDefault      B.11.23.0706    Select WBEM Providers
     VMProvider           A.03.00.76      WBEM Provider for Integrity VM
   ```

2. 若要列出已登錄的 CIM 提供者及其目前的狀態，以確定它們全部都已啟用，請執行下列指令：

   `# cimprovider -l -s`

   這時會顯示一長串提供者模組清單，讓您檢查它們是否全部都已啟用。

3. 執行下列指令，檢查 `OnlineDiag` 是否已安裝，並確定版本為 B.11.11.16xx 或以上版本。

   `# swlist | grep -i OnlineDiag`

   應該會傳回類似下列的輸出：

   ```
   # swlist | grep -i OnlineDiag
     OnlineDiag          B.11.23.10.02   HPUX 11.23 Support Tools Bundle, December
   2007
   ```

4. 執行下列指令，檢查 OnlineDiag 是否回報 `Event Monitoring is Currently Enabled`，且 EMS 版本為 A.04.20 或以上版本，而 STM 為 A.49.10 或以上版本：

   `# /etc/opt/resmon/lbin/monconfig`

   應該會傳回類似下列的輸出：

   ```
     EVENT MONITORING IS CURRENTLY ENABLED.
     EMS Version : A.04.20.23
     STM Version : C.58.00

   ==========================================================================
   --------------       Monitoring Request Manager Main Menu      -------------
   ==========================================================================

   Note: Monitoring requests let you specify the events for monitors
         to report and the notification methods to use.

   Select:
      (S)how monitoring requests configured via monconfig
      (C)heck detailed monitoring status
      (L)ist descriptions of available monitors
      (A)dd a monitoring request
      (D)elete a monitoring request
      (M)odify an existing monitoring request
      (E)nable Monitoring
      (K)ill (disable) monitoring
      (H)elp
      (Q)uit
      Enter selection: [s]
   ```

5. 選取 Q 結束 EMS Monitoring Request Manager Main Menu。
6. (選擇性) 執行下列指令，判斷 (選用，但建議) System Management Homepage (SMH) 元件至少為 A.2.2.6.2 版：

   ```
   # swlist SysMgmtWeb SysMgmtHomepage
   ```

   應該會傳回類似下列的輸出：

   ```
   # swlist SysMgmtWeb SysMgmtHomepage
   # Initializing...
   # Contacting target "hpux-01"...
   #
   # Target:  hpux-01:/
   #

   # SysMgmtWeb                                    A.2.2.6.2      HP-UX Web Based S
   ystem Management User Interfaces
   # SysMgmtWeb.SysMgmtHomepage                    A.2.2.6.2      HP-UX System Mana
   gement Homepage - Web-Based User Interfaces
     SysMgmtWeb.SysMgmtHomepage.SMH-UILIB          A.2.2.6.2      HP-UX System Mana
   gement Homepage User Interface Library
     SysMgmtWeb.SysMgmtHomepage.SMH-UILIB-COM      A.2.2.6.2      HP-UX System Mana
   gement Homepage User Interface Library (common files)
   [hpux-01]/var/adm/sw/products/OpenSSL
   #
   ```

9.6 在 CMS 上設定 WEBES 以支援 HP-UX 系統上的 WBEM 指示

完成下列步驟，設定 WEBES 以接收 WBEM 通訊：

1. 確認 HP-UX 系統已安裝所有必要的軟體 (如以上所列)。
2. 確定中央管理伺服器 (CMS) 已安裝 WEBES，且正在 Insight Remote Support Advanced A.05.40 環境中執行。
3. WEBES 會根據 HP SIM 所找到的資訊，自動針對 HP-UX 受管理系統建立 `WBEM 伺服器`類型的受管理實體。
4. WEBES 會從 HP SIM 取得其與受管理系統上的 HP-UX CIMOM 進行通訊時所需的資訊，並將該資料儲存在受管理實體中。當 WEBES 從 HP SIM 收到 WBEM 使用者名稱和密碼後，便會向 HP-UX 伺服器訂閱指示。

若要將 HP-UX 系統與 WBEM 一起新增至 HP SIM：

對任何 HP SIM 安裝而言，這個程序都是一樣的，都是使用 Internet Explorer 或 Mozilla 來連線至 HP SIM。

1. 透過瀏覽器登入 HP SIM。您必須具有系統管理權限才能新增系統。
2. 將 WBEM 認證新增至全域通訊協定設定。選取 **Options→Security→Global Protocol Settings**，在 WBEM 設定區段下新增 root/密碼認證。



附註： HP SIM 會要求對每一個 HP-UX 受管理系統將 root/密碼新增至 WBEM 通訊協定登入，但 WBEM 通訊也可以使用無權限的帳戶。

若要在 HP-UX 受管理系統上設定適當的無權限帳戶，請執行下列動作：

1. 建立使用者或使用現有的無權限使用者。指定的使用者名稱必須代表本機主機上有效的 HP-UX 使用者。在此範例中，您將建立一個名稱為 `sam` 的使用者，將該使用者指派至使用者群組，然後設定使用者密碼：

   `#useradd -g users sam`

   `#passwd sam` (出現提示時，提供密碼並確認)

   這是在 HP-SIM 中要針對此受管理系統的 WBEM 通訊而提供的使用者和密碼。

2. 檢閱目前的 CIM 設定，如下所示：

   `#cimconfig -l -p`

   輸出範例：

   ```
   sslClientVerificationMode=disabled
   enableSubscriptionsForNonprivilegedUsers=false
   shutdownTimeout=30
   authorizedUserGroups=
   enableRemotePrivilegedUserAccess=false
   enableHttpsConnection=true
   enableHttpConnection=true
   ```

3. 根據以上的輸出，在 CIM 計劃設定中確定/設定下列變數：

   ```
   #cimconfig -s enableSubscriptionsForNonprivilegedUsers=true -p
   #cimconfig -s enableNamespaceAuthorization=true -p
   ```

4. 停止後啓動 CIM 伺服器，以在 CIM 現行設定中設定設定變更

   ```
   #cimserver -s
   #cimserver
   ```

5. 確認 CIM 現行設定中的設定：

   `#cimconfig -l -c`

   輸出範例：

   ```
   sslClientVerificationMode=disabled
   enableSubscriptionsForNonprivilegedUsers=true
   shutdownTimeout=30
   authorizedUserGroups=
   enableRemoteprivilegedUserAccess=true
   enableHttpsConnection=true
   enableNamespaceAuthroization=true
   enablehttpConnection=false
   ```

6. 將使用者 sam 的讀取和寫入授權新增至每一個命名空間，包括 root/cimv2、root/PG_InterOp 及 root/PG_Internal：

   ```
   #cimauth -a -u sam -n root/cimv2 -R -W
   #cimauth -a -u sam -n root/PG_InterOp -R -W
   #cimauth -a -u sam -n root/PG_Internal -R -W
   ```

```
#cimauth -a -u sam -n root/cimv2/npar -R -W
#cimauth -a -u sam -n root/cimv2/vpar -R -W
```

7. 確認使用者的授權：

   輸出範例：

   ```
   sam, root/PG_InterOp, "rw"
   sam, root/PG_Internal, "rw"
   sam, root/cimv2, "rw"
   ```

---

3. 尋找系統。選取 **Options→Discovery**，再選取 **Manual Discovery**。
4. 新增系統名稱 (最好是完整的 DNS 名稱)。
5. (選擇的) 確認 HP SIM 已正確找到系統。簡單的作法是在 Search 面板中輸入系統的名稱，然後按一下 Search。搜尋完成時，選取系統，然後從功能表中選取 Properties (選取 Tools→System Information→Properties)，然後按一下 **Run Now**。產生的頁面包含只透過 WBEM 擷取的資料。
6. 在 HP-SIM 系統頁面中設定您的受管理系統時，請確認 Identification 標籤區段包含系統 Serial Number 和 Product Number 的值。如果這些欄位中沒有填入值，請按一下頁面頂端的 **Tools & Links** 標籤，然後選取並開啟 **Edit System Properties** 連結，接著在 Contract and Warranty Information 區段、Entitlement Information 子區段及 Customer Entered Serial Number 和 Customer Entered Product Number 欄位中輸入這些值。選取 **OK**，完成此更新。

   若要判斷 HP-UX 受管理系統的序號和產品號碼，可以存取伺服器的 MP、選取 Command Menu，然後使用 ID 指令 (如果是 cellular 行動伺服器) 或 PS 指令 (如果是非 cellular 行動伺服器)，以顯示此資訊。伺服器前方面板的系統識別外拉標籤上也印有此資訊。
7. 訂閱 WBEM 事件。從 All Systems 集合中，針對您要擷取其中指示的系統，選取每個系統左邊的核取方塊。選取 Options→Events→Subscribe to WBEM events，然後按一下 **Run Now**。工作隨即開始執行且應該會順利完成，沒有任何錯誤。
8. 傳送測試指示：您可以在受管理系統上產生測試事件，以確認一切都已正確設定。在受管理系統上執行下列指令：`# etc/opt/resmon/lbin/send_test_event disk_em`
9. 若要確認 HP SIM 已收到事件，您必須立即存取 HP SIM GUI。透過瀏覽器登入 HP SIM 來檢視 WBEM 指示。在 Systems and Events 面板中選取 All Events。Events→Event Type 之下有一個參考資訊事件，稱為 HP-UX EMS Disk Event。按一下此事件類型即可檢視詳細資訊。
10. 在 HP-UX 伺服器上發出測試事件來測試安裝，並確定 WEBES 已收到且顯示這些事件。

如需 SysFaultMgmt 的詳細資訊，包括在 HP-UX 上定義 WBEM 使用者/密碼帳戶並發出測試事件，請參閱下列文件：

- 《`HPUX System Fault Management Administration Guide`》(http://docs.hp.com/en/diag/sfm/5992-1318.pdf)
- 《`EVA CommandView Installation Guide`》(http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01080985/c01080985.pdf)

9.7 HP-UX 系統的防火牆/DMZ 連接埠需求

表 9-4 HP-UX 系統的防火牆/DMZ 連接埠需求

服務	通訊協定	來源 IP	目的地 IP	目的地連接埠
非 SNMP 問題討論區	http	McData/HAFM 交換器 DecEvent	CMS	2069
SNMP trap 傳遞	SNMP	受管理系統	CMS	162

表 9-4 HP-UX 系統的防火牆/DMZ 連接埠需求 (繼續)

服務	通訊協定	來源 IP	目的地 IP	目的地連接埠
HP-UX 事件監視				
WBEM 事件接收器	http/https	受管理系統	CMS	50004
HP SIM WBEM 指示設定	https	受管理系統	CMS	5989
HP-SIM GUI	https	任何瀏覽器	CMS	50000
Remote Support Configuration Collector				
儲存集合 - SSH	TCP	CMS	受管理系統	22
儲存集合 - Telnet	TCP	CMS	受管理系統	23
儲存集合 - (NSR) - http	http	CMS	受管理系統	80
儲存集合 - (EVA) - https	https	CMS	受管理系統	2372
儲存集合 - SNMP	SNMP/udp	CMS	受管理系統	161
儲存集合 - SMI-S	http	CMS	受管理系統	5988
儲存集合 - SMI-S	https	CMS	受管理系統	5989
儲存集合 SMH「喚醒」	http	CMS	受管理系統	2301
伺服器集合初始化 (SOAP)	https	CMS	受管理系統	2381
伺服器集合結果 (SOAP)	https	受管理系統	CMS	50001
UC 本機通訊 (SOAP) - (UC 至 WEBES sidbuilder)	https	CMS	CMS	7902
UC 本機通訊 (SOAP) - (GUI、CLI、MessageReceiver)	https	CMS	CMS	20649
UC 本機通訊 (SOAP) - (UC 至 JBoss 的伺服器集合初始化)	https	CMS	CMS	50001

9.8 設定用於主動式收集服務的 HP-UX 受管理系統

HP-UX 受管理系統上需要進階設定收集器 (ACC)，才能針對有資格的客戶收集設定、可用性及效能資料。本節說明安裝 ACC 及其他必要設定所需的程序，以便備妥 HP-UX 受管理系統來啓用主動式支援服務。

9.8.1 下載並安裝伺服器集合 Client



附註： 此時應該已安裝 System Management Homepage 必要條件。

ACC 元件做爲本機代理程式使用，讓 Remote Support Configuration Collector 能夠從您的合格 HP-UX 受管理系統收集設定資料。HP-UX 伺服器的進階設定收集器 (ACC) 元件可在 CMS 上透過 HP Software Manager (RSSWM) 取得。必須分送此元件並安裝至您的 HP-UX 受管理系統。

.

ACC 軟體壓縮在 GZIP 檔案中，以 SD-UX 系列軟體庫的形式來分送。RSSWM 會將檔案傳送至 CMS 上的下列其中一個預設位置：

`c:\Hewlett-Packard\BusinessSupport\UC\ACC-HPUX\`

或

`c:\Program Files[(x86)]\SWMAgent\Installers\UC\ACC-HPUX`

或

`c:\Program Files\HP\SWMAgent\Installers\UC\ACC\HPUX`



附註： 在 HP SIM 5.3 中，當您安裝 HP Remote Support Software Manager 時，可設定此目錄。

如果是 Insight Remote Support Advanced A.05.40，則可用的檔案如下：

- PA-RISC 軟體庫：

  `rs-acc-hpux 11.x-PA-A.05.40.xxx.depot.gz`

- Itanium 軟體庫：

  `rs-acc-hpux 11.x-IA-A.05.40.xxx.depot.gz`

針對這兩種 A.05.40 檔案，您應該根據受管理系統的處理器類型來選擇並傳送適當的檔案。

由於每一個客戶的環境都不相同，可將此檔案分送至 HP-UX 受管理系統的方法眾多，本指南將不詳列所有可能的方法。不過，最簡單的作法是登入中央管理伺服器 (CMS) 並使用 FTP，將檔案傳送至受管理系統上的暫存位置。

依照指示安裝 RS-ACC 組合：



附註： 以下的 `filename` 執行個體代表變數。實際的檔名視您已下載的軟體庫及您是否重新命名檔案而定。

- 解壓縮從 CMS 複製的軟體檔案：

  `gunzip filename.depot.gz`

- 從已解壓縮的軟體庫檔案來安裝軟體：`swinstall -s $PWD/filename.depot RS-ACC`

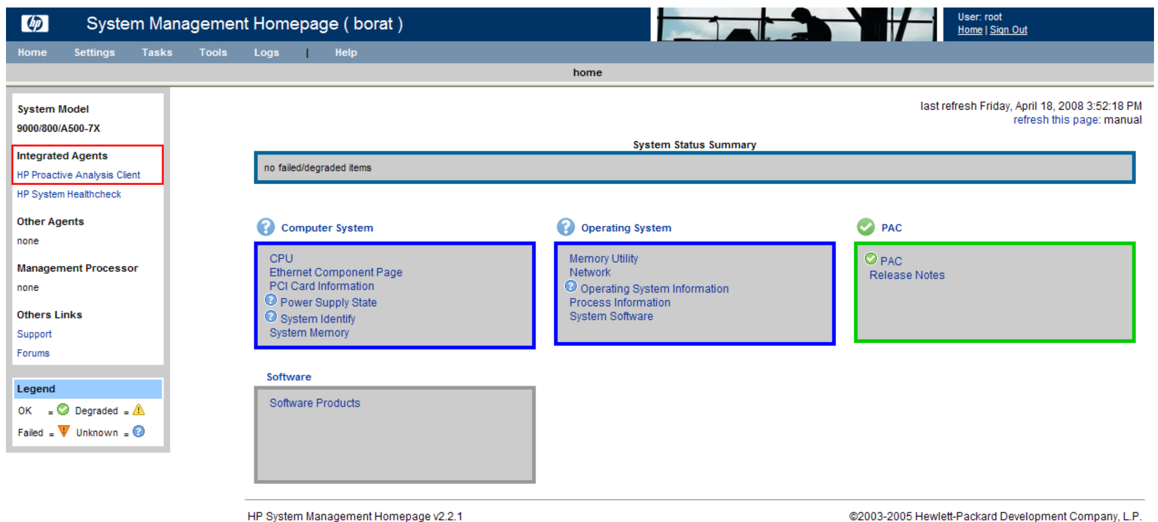
以下是已安裝之組合的 swlist 範例 (版本號碼不是最新的)：

```
# RS-ACC                  A.05.10.15.047 HP Remote Support Advanced Configuration Collector
  RS-ACC.UC-ACC           A.05.10.15.047 HP Remote Support Advanced Configuration Collector
  RS-ACC.MCPS-PAC         A.01.00.00.183 Proactive Client
  RS-ACC.MCPS-AVC         A.02.03.00.00213 HP Availability Collector
  RS-ACC.MCPS-COMMON      A.01.04.00     HP Service Mission Critical Common Component
|
```

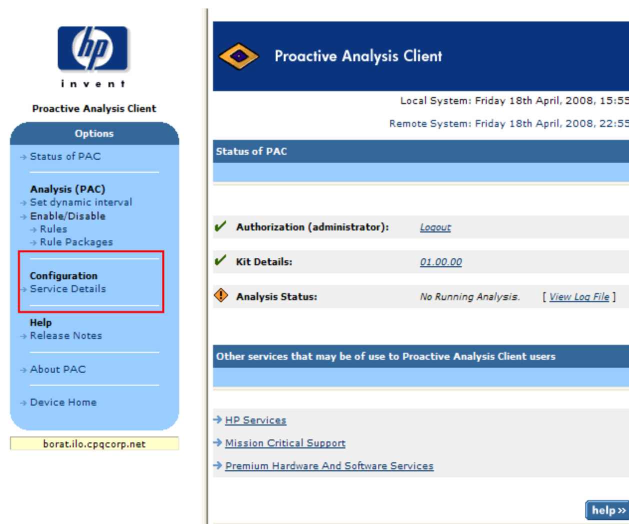
9.8.2 設定 System Management Homepage (SMH) 來支援自訂的 Performance Collections

如果您是客戶的 HP 客服小組成員，且想要修改在 Performance Collections 上執行的分析長度或類型以自訂報告，則需要透過 HP-UX 受管理系統上的 System Management Homepage (SMH) 來更新 **Specialist E-mail**。若要變更密碼，請執行下列動作：

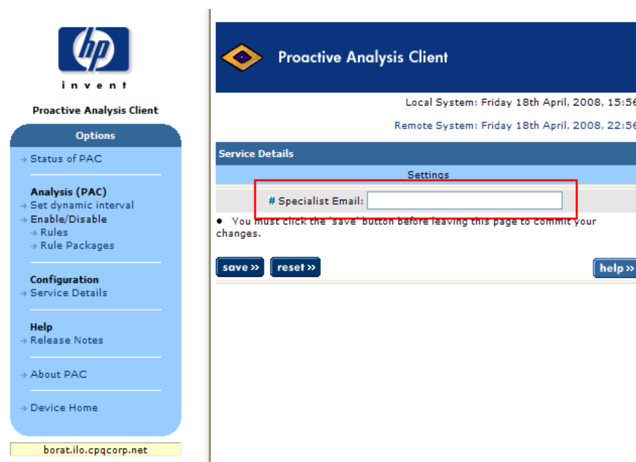
1. 存取 HP-UX 受管理系統上的 System Management Homepage
2. 在 SMH 視窗的 **Integrated Agents** 區段下，按一下 **HP Proactive Analysis Client** 選項。



3. 在視窗的 **Configuration** 區段下，按一下 **Service Details** 選項。



4. 在欄位中輸入正確的 Specialist 電子郵件地址，然後按一下 **Save**。



5. 關閉 System Management Homepage 和 HP Proactive Analysis Client 視窗。

現在，依照《HP Insight Remote Support Advanced CMS 設定與使用手冊》中的指示完成 CMS 設定。

10 OpenVMS 受管理系統的 Insight Remote Support Advanced 支援使用前提

10.1 安裝或升級必要軟體「之前」必要的受管理系統狀態

在將受管理系統升級以搭配 CMS 上安裝的 Insight Remote Support Advanced A.05.40 版一起使用時，您「必須移除所有」目前可能已安裝的舊版 WEBES 或 HP ISEE Client。另外，也必須移除原本稱為 WCCProxy 的 Event Log Monitoring Collector (ELMC)，但在解除安裝 WEBES 時也會自動將它一併解除安裝。

10.1.1 準備 OpenVMS 受管理系統

「唯有」當您在受管理系統上已安裝「任何」版本的 HP ISEE Client、WEBES 或 ELMC 時，才需要進行這些步驟。

10.1.1.1 從 OpenVMS 受管理系統中移除 HP ISEE

「唯有」當您在受管理系統上已安裝 HP Instant Support Enterprise Edition (ISEE) 時，才需要進行這些步驟。如果您沒有在受管理系統上安裝 ISEE，可以跳過這一節。



重要： Instant Support Enterprise Edition (ISEE) A.03.95 及舊版與 Insight Remote Support Advanced「不是相同的應用程式」，請不要安裝在任何受管理系統上。

若要移除 ISEE，請完成下列步驟：

1. 關閉任何正在執行 ISEE Client 使用者介面的瀏覽器。
2. 登入受管理系統。
3. 若要從系統中移除 HP ISEE 軟體，請執行下列指令：

   ```
   $ PRODUCT REMOVE ISEE
   ```

4. ELMC (WCCProxy) 由 ISEE 及其他工具共用，例如 WEBES。為了確保使用 WCCProxy 的工具維持在正確的數量，在移除 ISEE 之後，請在受監視系統上執行下列指令：

   ```
   $ @WCCPROXY_COMMON:[COMMON.WCCPROXY.BIN]WCCPROXY_INSTALL UNINSTALL
   MASTERISEE
   ```

   如果還有其他任何工具在使用 WEBES，WCCProxy 會降低工具參考計數。此計數儲存在 `WCCPROXY_COMMON:[COMMON.WCCPROXY]REF.CNT` 檔案中。

   接著會顯示下列文字：

   ```
   WCCProxy is still in use by other applications on this system.
   Uninstallation of the last using application will also remove the
   WCCProxy.
   This Kit will decline deletion.
   ```

   這是 WCCProxy 的正常行為。即使 WCCProxy 不會移除自己，您也必須執行這個指令，讓 WCCProxy 知道 ISEE 已不再使用它。如果 ISEE 是僅存正在使用 WCCProxy 的工具，則 WCCProxy 會移除自己，並顯示類似下列的文字：

   ```
   WCCProxy is being uninstalled.
   The following product has been selected:
      DEC AXPVMS WCCPROXY V1.x-x Layered Product
   The following product will be removed from destination:
   DEC AXPVMS WCCPROXY V1.x-x DISK$ALPHASYS:[SYS0.SYSCOMMON.]
   ```

```
Portion done:
0%...20%...30%...40%...50%...60%...70%...80%...90%...100%

The following product has been removed:
   DEC AXPVMS WCCPROXY V1.x-x Layered Product
```

10.1.1.2 從 OpenVMS 受管理系統中移除 WEBES

若要從 OpenVMS 受管理系統中移除 WEBES，請執行下列動作：

1. 重新執行安裝指令，如下所示：

   ```
   $ @svctools_home:[common.bin]webes_install

   WEBES UPDATE - MAIN MENU
   ========================

    1. SEA Menu
    2. CCAT Menu
    3. Start At Boot Time
    4. Customer Information
    5. System Information
    6. Service Obligation
    7. Start DESTA Director
    8. Stop DESTA Director
    9. Uninstall Webes
       - Fully uninstalls Webes and all installed dependent components
         such as SEA and CCAT
   10. Exit
   =========================
   ```

2. 從更新功能表中選擇 Uninstall WEBES 選項，並依照出現的提示進行。

10.1.2 OpenVMS 受管理系統的 Insight Remote Support Advanced 支援需求

System Event Analyzer (SEA) 是遠端系統事件監視工具，也是在 CMS 上執行的 WEBES 元件。

錯誤記錄檔：安裝之後，CMS上的WEBES會開始分析目前儲存在錯誤記錄檔中的所有事件，並使用 OpenVMS 系統上安裝的 ELMC 來收集事件，這會導致 CPU 使用率長時間偏高。若要控制這項操作，建議您在安裝之前封存並清除錯誤記錄檔案，如下列指示所述。這樣可以縮小記錄檔的大小，並能縮短初始掃描所需的時間。

請依照下列準則來清除錯誤記錄檔。在清除記錄檔時，即使ELMC已安裝且正在執行，您也不需要停止後再重新啓動 Director 程序。另外，請不要停用後再重新啓動 ERRFMT 系統事件記錄程序。

預設錯誤記錄檔 (通常是 `SYS$SYSROOT:[SYSERR]ERRLOG.SYS`) 會不斷變大並保留在系統磁碟上，直到使用者明確地將它重新命名或刪除爲止。重新命名或刪除記錄檔時，系統會在大約15分鐘之後，建立新的、乾淨的錯誤記錄檔。



小心： 重新命名或刪除現有的記錄檔之後，請不要在還沒出現新的預設記錄檔之前安裝ELMC。

如果您重新命名記錄檔，則稍後可以分析已儲存的記錄檔。

排定的維護：除了在安裝 SEA 之前開始使用全新的記錄檔，您也可以對錯誤記錄檔定期執行維護。作法之一是每天都重新命名 ERRLOG.SYS。例如，您可以在每天早上 9:00 將 ERRLOG.SYS 重新命名爲 ERRLOG.OLD。爲了釋出系統磁碟上的空間，您可以將已重新命名的版本備援至不同的磁碟區，然後從系統磁碟刪除該檔案。

10.1.2.1 滿足 OpenVMS 受管理系統的 ELMC 一般需求

受管理系統必須符合下列基本需要，您才能安裝 ELMC。在 cluster 內，cluster 的每個節點都適用下列最低需求：

10.1.2.1.1 系統需求

- 處理器架構：HP AlphaServer 或 Integrity (Itanium) 伺服器
- 作業系統 OpenVMS Alpha - 7.3-2 或更高版本
- 作業系統 OpenVMS Itanium (Integrity) - 8.2–1 或更高版本
- 可用磁碟空間最少 20,000 個區塊。

10.1.2.1.2 安裝條件和需求

- 連線能力：必須安裝並執行 TCP/IP。

  即使已停止對其他機器傳送 TCP/IP 流量，仍然必須啓用將本機主機名稱解析成 IP 位址的功能。否則，Director 就無法正確處理 ELMC 訊息流量，也無法啓動。

  ELMC 只正式支援兩個用於 OpenVMS 的 TCP/IP 產品：

  — HP TCP/IP Services for OpenVMS 5.4 版或更高版本

  — Process Software MultiNet (不是 TCPware)

  附註： 其他 TCP/IP 產品也可能沒有問題，所以不論安裝什麼 TCP/IP 產品 (如果有的話)，WEBES 安裝套件一定會完成。

- LOCALHOST 項目：爲了讓 ELMC 正常運作，OpenVMS TCP/IP HOSTS 資料庫中必須定義 LOCALHOST 項目。依預設會正確定義，但可以移除，不過這樣會導致 WEBES 失敗。

  輸入下列指令：

  ```
  $ TCPIP SHOW HOST /LOCAL
  ```

  尋找 LOCALHOST，IP 位址應該是 127.0.0.1。如果清單中沒有出現 LOCALHOST，請輸入下列指令：

  ```
  $ TCPIP SET HOST LOCALHOST /ADDRESS=127.0.0.1 /ALIAS=LOCALHOST
  ```

  輸入 ping 指令來確認已新增 LOCALHOST：

  ```
  $ TCPIP PING LOCALHOST
  PING LOCALHOST (127.0.0.1):56 data bytes
  64 bytes from 127.0.0.1:icmp_seq=0 ttl=64 time=0 ms
  64 bytes from 127.0.0.1:icmp_seq=1 ttl=64 time=0 ms
  64 bytes from 127.0.0.1:icmp_seq=1 ttl=64 time=0 ms
  ```

  確認 `LOCALHOST` 有回應 ping 指令之後，您就可以利用 Ctrl-C 或 Ctrl-Y 來停止 ping。

- 系統韌體：根據 FRU 表格版本 5 規格，必備的系統韌體支援事件的記錄，這也是 WEBES FRU 設定樹狀結構處理所需要的。

  All DSxx 和 ES40 系統必須具有韌體 5.7–4 版或更高版本。

  System Event Analyzer 所支援的其他所有產品 (請參閱《WEBES 版本注意事項》) 都隨附已經與 WEBES/SEA 處理相容的韌體版本。

  一般而言，使用者應該取得其平台可用的最新韌體版本，以享受最新的改進功能。

- 驗證序號 (僅具有 SEA 元件的一些 GS80、GS160 及 GS320 系統才需要)

  某些 GS80、GS160 及 GS320 系統在出廠時並未正確設定系統序號，而 CMS 上的 SEA 規則必須在序號正確設定時才有作用。

  受影響的序號以字母 G 作爲開頭。

  在 SRM 主控台韌體提示字元上 (首次啓動系統時出現的提示字元)，利用下列指令來檢查序號：

  ```
  show sys_serial_num
  ```

  顯示的序號應該符合電源箱中機型/序號標籤上的實際序號。必要的話，請利用下列指令來變更序號：

set sys_serial_num

輸入電源箱標籤上所顯示的六位序號。

多部 AlphaServer

在訂購多部 AlphaServer 時，也可能會發生這種問題，因爲工廠可能將相同的序號指派給每個系統。在此情況下，SEA 規則就無法正確運作，因爲它們需要每一部 AlphaServer 都有唯一的編號。如果是這種情形，當您使用 set sys_serial_num 指令時，請在序號後面加上 –1、–2、–3 等依此類推，以唯一地識別每一部 AlphaServer。

分割區 Partitions

請注意，在同一部 AlphaServer 上，多個 Partitions 一定都有相同的序號，因爲它們都在同一部機器上。在此情況下，SEA 沒有衝突問題，所以請不要嘗試將不同序號指派給同一部機器上的不同 Partitions。

10.1.2.1.3 必要的權限和存取權

- 使用者需要具備下列所有 OpenVMS 權限，才能安裝或解除安裝 ELMC：
  - ALTPRI
  - BUGCHK
  - BYPASS
  - CMKRNL
  - DIAGNOSE
  - IMPERSONATE
  - NETMBX
  - OPER
  - SYSLCK
  - SYSPRV
  - TMPMBX

  在解除安裝 WEBES 時，執行解除安裝的使用者必須使用原本安裝 WEBES 時的相同使用者名稱。

  唯有當 cluster 是由單一系統磁碟來提供服務時，SET PROCESS 指令才能對所有 cluster 節點設定權限。不過，在具有多個系統磁碟的 cluster 上，您可能會選擇在由其他系統磁碟提供服務的節點上安裝 WEBES，而不是安裝在您正在安裝的系統磁碟提供服務的節點上。在此情況下，SET PROCESS 不會在那些節點 (由其他系統磁碟提供服務的節點) 上設定權限，且 WEBES 也無法正確安裝在那些節點上。

  爲了正確安裝在具有多個系統磁碟的 cluster 上，請在您想要安裝 ELMC 的所有節點上將必要權限設爲預設值 (您登入時所取得的權限)，而不要使用 SET PROCESS 指令。

  關於一個與多個系統磁碟的比較，如需其他相關的注意事項，請參閱「共用的非系統磁碟安裝」一節。

  執行 ELMC

  使用者需要具備下列所有 OpenVMS 權限，才能執行任何 ELMC 指令。請注意，這些只是安裝、升級或解除安裝 ELMC 所需的一部分權限：

  - ALTPRI
  - BUGCHK
  - CMKRNL
  - DIAGNOSE
  - IMPERSONATE
  - NETMBX
  - SYSPRV
  - TMPMBX

- cluster 節點對安裝目錄的存取權

  cluster 節點必須能夠存取您選擇安裝 ELMC 的目標目錄，安裝套件才會安裝在 cluster 節點上。換言之，該節點必須裝載含有目標目錄的磁碟。這表示安裝不見得會在所有 cluster 節點上都安裝 ELMC，因爲不是所有節點都能夠識別要安裝 ELMC 的位置。

  下列範例會說明這個問題：

  — cluster：所有節點都共用相同的系統磁碟。

    安裝節點：任何節點

    安裝目標：預設位置 SYS$COMMON:[HP...]

    結果：ELMC 本身安裝在所有節點上。

  — cluster：兩個節點除外，其他所有節點都共用系統磁碟 A。這兩個節點共用系統磁碟 B。

    安裝節點：使用系統磁碟 A 的節點。

    安裝目標：預設位置 SYS$COMMON:[HP...]

    結果：其他兩個節點不會有 ELMC。

    在上述例子中，您可以從任一節點執行安裝，且同樣選擇預設位置 SYS$COMMON:[HP...]，對其餘的兩個節點再安裝一次 ELMC。請注意，這是完全獨立的 ELMC 安裝，與第一次在大多數節點上安裝不同。

  — cluster：兩個節點除外，其他所有節點都共用系統磁碟 A。這兩個節點共用系統磁碟 B。所有節點也都裝載非系統磁碟 C。

    安裝節點：任何節點

    安裝目標：磁碟 C 上的目錄，由您在安裝期間指定。

    結果：ELMC 本身安裝在所有節點上。



附註： 在所有情況下，安裝套件也都可讓您選擇只有一部分節點才能看到安裝位置。

10.1.2.2 在 OpenVMS 受管理系統上安裝 ELMC 軟體套件

非系統而共用的磁碟之安裝

OpenVMS cluster 可以包含由單一通用系統磁碟提供服務的節點，也可以包含由多個系統磁碟提供服務的節點。任何給定的節點都只由一個系統磁碟提供服務，但一個系統磁碟可以提供服務給一或多個節點。每一個系統磁碟都包含自己的 PCSI 資料庫 (產品登錄)。

ELMC 可以安裝在系統磁碟上，也可以安裝在非系統磁碟上。不過，由不同系統磁碟提供服務的多個節點可以存取一個共用的非系統磁碟。這表示 ELMC 不限於只能安裝在由一個給定系統磁碟提供服務的節點上。不過，一個 PCSI 資料庫只能屬於一個系統磁碟。

這種情形可能會在 PRODUCT SHOW PRODUCT WEBES 指令中產生差異。根據原本安裝 WEBES 的節點 (即安裝節點)，如果從由相同系統磁碟提供服務的節點上執行這個指令時，則一律會顯示已安裝 ELMC。這是因爲 ELMC 安裝程式只會將 ELMC 登錄至提供服務給安裝節點的系統磁碟上的 PCSI 資料庫，而不會登錄至其他任何 PCSI 資料庫。如下圖所示，可能會產生兩種誤導的資訊。

- 如果某個節點與安裝節點都由同一個系統磁碟提供服務，但使用者並沒有將 ELMC 新增至該節點，則該指令會顯示已安裝 ELMC，但實際上並未安裝。
- 相反也，如果某個節點與安裝節點分別由不同的系統磁碟提供服務，且使用者已將 WEBES 新增至該節點，則該指令不會顯示已安裝 WEBES，但實際上已安裝。

解壓縮安裝軟體套件

若要解壓縮 ELMC 安裝套件，請將 .EXE 可執行檔放在如下的目錄中：

- 目錄中沒有其他套件，尤其是其他版本的 WEBES 套件。
- 目錄中沒有先前操作所遺留的舊版 WEBES 或 WCC 檔案 (最可靠的作法就是使用空目錄)。

然後，輸入下列指令：

```
$ run ELMC_{version}.EXE
```

這個指令會解壓縮 ELMC 安裝檔案。

執行 ELMC OpenVMS 安裝

確定符合上述所有指示之後，請執行安裝指令並依照提示進行。



附註： 這個指令會在目前的目錄中執行 DCL 指令檔 WCCPROXY_INSTALL.COM。請不要執行 PRODUCT INSTALL WCCPROXY 指令，這個指令通常是用來安裝以 PCSI 爲基礎的產品。這個指令會中止並提示您改爲執行 WCCPROXY_INSTALL 指令檔。將預設目錄設爲含有 wccproxy_install.com 檔案的目錄，在上一步解壓縮 ELMC .exe 檔案時已建立此檔案。

執行 DCL 指令檔：

```
$ @wccproxy_install install
```

套件會開始安裝並完成，不會提示使用者。當傳回 DCL 提示字元 ($) 時，即表示安裝已完成，而 ELMC (WCCProxy) 程序會開始執行。

10.2 在 WEBES 使用者介面中更新 ELMC 通訊協定

因爲 WEBES 會自動安裝在 CMS 上，之後 ELMC 儲存庫套件才能分送並安裝在受管理系統上，所以您需要登入 CMS 上的 WEBES 介面並修改通訊協定來包含 ELMC。請在您的 CMS 上完成下列步驟：

1. 開啓 System Event Analyzer 介面：

   開始 → 程式集 → Hewlett-Packard Service Tools → Service Event Analyzer → Service Event Analyzer

2. 在畫面頂端的工具列上，按一下 **Configure Webes Managed Entities** 圖示。



3. 從清單中選擇您的受管理系統，然後按一下主機名稱連結。
4. 在 Managed Entity Properties 畫面上，從下拉式功能表中選擇啓用 ELMC。

Managed Entity Properties

Setting	Value
User-Definable Entity Name	.hp.com
Entity Name on the Network	.hp.com
System Type	ManagedSystem
System Subtype	ProLiant
ELMC	off (disabled / off / DefaultELMC / defaultCommandView)
SNMP	
WBEM	
Warranty Check	Check
Entitlement type	Warranty
Entitlement Serial Number	US
Entitlement Product Number	3
Entitlement ID	
Obligation ID *Customers in North and Latin America with Compaq Contract ID or HP CarePack entitlement should enter their Compaq Software Obligation ID (if any) as well:*	
Custom Delivery ID	
Physical Location	

5. 套用變更並關閉 System Event Analyzer。

11 可獲得 Insight Remote Support Advanced 支援之 Tru64 Unix 受管理系統的需求

11.1 安裝或升級必要軟體「之前」必要的受管理系統狀態

在 CMS 上升級受管理系統以搭配 Insight Remote Support Advanced A.05.40 版一起使用時，您「必須移除所有」目前可能已安裝的舊版 WEBES 或 HP ISEE Client。另外，也必須移除原本稱為 WCCProxy 的 Event Log Monitoring Collector (ELMC)，但在解除安裝 WEBES 時也會自動將它一併解除安裝。

11.1.1 從 Tru64 UNIX 受管理系統中移除 HP ISEE

「唯有」當您在受管理系統上已安裝 HP Instant Support Enterprise Edition 時，才需要進行這些步驟。如果您沒有在受管理系統上安裝 ISEE，可以跳過這一節。



重要： Instant Support Enterprise Edition (ISEE) A.03.95 及舊版與 Insight Remote Support Advanced「不是相同的應用程式」，請不要安裝在任何受管理系統上。

若要移除 ISEE，請完成下列步驟：

1. 以 `root` 身分 (系統管理權限) 登入受監視系統。
2. 切換至您安裝 HP ISEE 時所建立的目錄 (cd) `/usr/ISEEInstall`。
3. 若要從系統中移除 HP ISEE 軟體，請執行下列指令：

```
./ISEEuninstall.sh
```

11.1.2 從 Tru64 UNIX 受管理系統中移除 WEBES

若要從 Tru64 UNIX 受管理系統中解除安裝 WEBES，請執行互動式 `/usr/sbin/webes_install_update` 公用程式、選擇移除所有 WEBES 的選項，並依照任何出現的提示進行。在 cluster 中，解除安裝會從 cluster 中的所有節點移除 WEBES。

11.2 滿足 Tru64 受管理系統的 ELMC 一般需求

受管理系統必須符合下列基本需要，您才能安裝 ELMC。在 cluster 內，cluster 的每個節點都適用下列最低需求：

11.2.1 系統需求

- 處理器架構：HP AlphaServer
- 作業系統 Tru64 UNIX 4.0F、4.0G、5.1A 版或更高版本



附註： 請注意，HP Sustaining Engineering 會維護一份支援 Tru64 UNIX 作業系統的排程。HP 不承諾支援以下產品：在已超過其支援最終日期之作業系統版本上安裝的 WEBES。請參閱下列 URL：http://www.hp.com/hps/os/os_pvs_amap.htm

- 最少需要 20 MB 的可用磁碟空間，才能安裝所有元件。

11.2.2 可獲得 Insight Remote Support Advanced 支援之 Tru64 Unix 受管理系統的需求

在 Tru64 Unix 受管理系統上安裝 ELMC 軟體之前，請先完成下列各節：

11.2.2.1 封存並清理錯誤記錄檔

System Event Analyzer (SEA) 是遠端系統事件監視工具，也是在 CMS 上執行的 WEBES 元件。如果想要 SEA 自動分析系統的原生錯誤記錄檔，您必須在支援的 HP 硬體平台或包含支援之 HP I/O 裝置的機器上進行安裝。請參閱《WEBES 版本資訊》，以取得支援的產品清單。

安裝之後，CMS 上的 WEBES 會開始分析目前儲存在錯誤記錄檔中的所有事件，並使用 Tru64 UNIX 系統上安裝的 ELMC 來收集事件，這會導致 CPU 使用率長時間偏高。若要控制這項作業，建議您首先依本節所述，封存並清除錯誤記錄檔，然後再安裝 ELMC。這樣可以縮小記錄檔的大小，進而節省初始掃描的負荷。

如果您決定清理記錄檔時 WEBES 已安裝且正在執行，請先停止 Director 程序，再開始此程序 (請參閱《SEA User Guide》，以取得停止 Director 的資訊)。一旦封存並清除錯誤記錄檔之後，即可使用《SEA User Guide》(可於 http://h18023.www1.hp.com/support/svctools/webes/index.html 上取得) 中的程序，重新啓動 Director。

11.2.2.1.1 4.0F

1. 停止 binlogd 程序：`# /sbin/init.d/binlog stop`
2. 如果需要，請將原始的錯誤記錄檔移至任何適當的名稱，例如：

   ```
   # mv /var/adm/binary.errlog /var/adm/binary.errlog.2002_06_11
   ```

   儲存的記錄可留待以後進行進一步分析。
3. 如果您略過步驟 2，請移除原始的錯誤記錄檔：`# rm /var/adm/binary.errlog`
4. 重新啓動系統。重新啓動期間，系統會建立新的 binary.errlog 檔案，其中包含新的設定事件。系統也會重新啓動 binlogd 程序。

11.2.2.1.2 4.0G

1. 停止 binlogd 程序：# /sbin/init.d/binlog stop
2. 如果需要，請將原始的錯誤記錄檔移至任何適當的名稱，例如：

   ```
   # mv /var/adm/binary.errlog /var/adm/binary.errlog.2002_06_11
   ```

   儲存的記錄可留待以後進行進一步分析。
3. 如果您略過步驟 2，請移除原始的錯誤記錄檔：`# rm /var/adm/binary.errlog`
4. 重新啓動 binlogd 程序：`# /sbin/init.d/binlog start`

11.2.2.1.3 5.A 或更高版本

引進了新的功能，可將訊號傳送至 binlogd，以儲存目前的記錄檔並建立新的記錄檔，而不需停止此程序。請遵循下列「確認 binary.errlog CDSL」和「在執行 binlogd 期間清除記錄檔」章節中的步驟。

11.2.2.1.3.1 確認 binary.errlog CDSL

在 5.1A 版或更高版本中，二進位錯誤記錄檔 /var/adm/binary.errlog 應該是指向每個 cluster 節點專屬檔案的「與內容關聯的符號連結」(CDSL)。這樣可確保每個節點上的binlogd程序會將該節點的事件儲存至其本身節點專屬的錯誤記錄檔/var/cluster/members/{memb}/adm/binary.errlog。

如果 CDSL 遭到刪除，binlogd 還是可以重新將它建立為標準的 cluster 通用檔案，但是它不會正確運作。若要檢查您的檔案，請發出下列指令：

```
# ls -l /var/adm/binary.errlog
```

正確的輸出看起來類似下列指令行：

```
>lrwxrwxrwx 1 root adm 43 Jun 11 12:54 /var/adm/binary.errlog -> ../
cluster/members/{memb}/adm/binary.errlog
```

不正確的輸出不會顯示 -> 連結指標：

```
-rw-r----- 1 root adm 560 Jun 11 12:59 /var/adm/binary.errlog
```

如果需要，請執行下列步驟來更正檔案：

1. 藉由在每個節點上發出下列指令，來停止所有 cluster 節點上的 binlogd 程序：

   ```
   # /sbin/init.d/binlog stop
   ```

2. 儲存的記錄可留待以後進行進一步分析。如果需要，請將原始的錯誤記錄檔移至任何適當的名稱，例如：

   ```
   # cd /var/adm
   # mv binary.errlog binary.errlog.2002_06_11
   ```

3. 針對您希望儲存之任何節點特定的錯誤記錄檔，來發出類似的移動指令，例如：

   ```
   # mv /var/cluster/members/{memb}/adm/binary.errlog
   /var/cluster/members/{memb}/adm/binary.errlog.2002_06_11
   # mv /var/cluster/members/{memb}/adm/binlog.saved/binary.errlog.saved
   /var/cluster/members/{memb}/adm/binlog.saved/
   binary.errlog.saved.2002_06_11
   ```

4. 移除現有的錯誤記錄檔，略過任何 **No such file or directory** 錯誤：

   ```
   # rm /var/adm/binary.errlog
   # rm /var/cluster/members/{memb}/adm/binary.errlog
   # rm /var/cluster/members/{memb}/adm/binlog.saved/binary.errlog.saved
   ```

5. 建立 CDSL：

   ```
   # mkcdsl /var/adm/binary.errlog
   ```

6. 藉由在每個節點上發出下列指令，來重新啟動所有 cluster 節點上的 binlogd 程序：

   ```
   # /sbin/init.d/binlog start
   ```

11.2.2.1.3.2 在執行 binlogd 期間清除記錄檔

如爲 5.1A 版或更高版本，請在您要清除的每個 cluster 節點上遵循下列步驟進行：

1. 確認已完成 binary.errlog CDSL 區段，如前所述。
2. 如果需要，請保留任何先前儲存的副本，以免因將其移動至任何適當名稱之後遭到覆寫，例如：

   ```
   # cd /var/cluster/members/member/adm/binlog.saved
   # mv binary.errlog.saved binary.errlog.2002_06_11
   ```

3. 導致 binlogd 複製並清除原始的錯誤記錄檔：

   ```
   # kill -USR1 `cat /var/run/binlogd.pid`
   ```

   先前的指令不會刪除 binlogd 程序。取而代之的是，它會傳送訊號給導致它將 /var/adm/binary.errlog 複製到 /var/cluster/members/member/adm/binlog.saved 的 binlogd。接著，系統會重新建立原始的 /var/adm/binary.errlog 檔案，其中只包含一個設定事件。請注意，/var/adm/binary.errlog 是一個會指向 /var/cluster/members/{memb}/adm/binary.errlog 的 CDSL。

如需進一步的詳細資訊 (包括如何使這類錯誤記錄檔管理自動化)，請參閱 binlogd 首頁上「Managing the Binary Error Log File」中的章節。

11.2.2.2 序號驗證

在 GS80、GS160 及 GS320 系統上，在受管理系統上安裝 ELMC 之前，請先確認序號與所指示的相同。

某些 GS80、GS160 及 GS320 系統在出廠時並未正確設定系統序號，而 CMS 上的 SEA 規則必須在序號正確設定時才有作用。受影響的序號以字母 G 作爲開頭。

在 SRM 主控台韌體提示字元上 (首次啓動系統時出現的提示字元)，利用下列指令來檢查序號：

```
show sys_serial_num
```

顯示的序號應該符合電源箱中機型/序號標籤上的實際序號。必要的話，請利用下列指令來變更序號：

set sys_serial_num

輸入電源箱標籤上所顯示的六位序號。

- 多部 AlphaServer：在訂購多部AlphaServer時，也可能會發生這種問題，因為工廠可能將相同的序號指派給每個系統。在此情況下，SEA 規則就無法正確運作，因為它們需要每一部 AlphaServer 都有唯一的編號。如果是這種情形，當您使用 set sys_serial_num 指令時，請在序號後面加上 –1、–2、–3 等依此類推，以唯一地識別每一部 AlphaServer。
- Partitions 分割區 在同一部 AlphaServer 上，多個 Partitions 一定都有相同的序號，因為它們都在同一部機器上。在此情況下，SEA 沒有衝突問題，所以請不要嘗試將不同序號指派給同一部機器上的不同 Partitions。

11.2.2.3 滿足 Tru64 Unix 受管理系統的 ELMC 一般需求

系統必須符合下列基本需要，您才能安裝 ELMC。在 cluster 內，cluster 的每個節點都適用下列最低需求：

11.2.2.3.1 系統需求

- 處理器架構：HP AlphaServer
- 作業系統：Tru64 UNIX 4.0F、4.0G、5.1A 版或更高版本

  請注意，HP Sustaining Engineering 會維護一份支援 Tru64 UNIX 作業系統的排程。HP 不承諾支援以下產品：在已超過其支援最終日期之作業系統版本上安裝的 WEBES。請參閱下列 URL：http://www.hp.com/hps/os/os_pvs_amap.htm
- 最少需要 20 MB 的可用磁碟空間，才能安裝所有元件
- 必須安裝並執行 TCP/IP 服務。

11.2.2.3.2 安裝條件需求

- 如果您具備使用 SLI2 程式設計介面的 EMX LP6000、LP7000 或 LP8000 介面卡 (KGPSA–xx)，請升級至 Emulex (EMX) 驅動程式的 1.22 版或更高版本。使用早於 1.22 版的 EMX 驅動程式可能會導致資料未正確處理。
- 系統韌體：根據 FRU 表格版本 5 規格，必備的系統韌體支援事件的記錄，這也是 WEBES FRU 設定樹狀結構處理所需要的。
  — All DSxx 和 ES40 系統必須具有韌體 5.7–4 版或更高版本。
  — 所有的其他系統 (目前是 ES45、GSxx 及 TS202c) 均隨附已可與 WEBES 處理相容的韌體版本。

  一般而言，使用者應該取得其平台可用的最新韌體版本，以享受最新的改進功能。

11.2.2.3.3 必要的權限和存取權

若要安裝、升級或解除安裝 WEBES，您必須以 root 使用者的身分登入。/usr/opt/hp/svctools 目錄是由 root 所擁有，並擁有 root (擁有者) 的 rwx (讀取、寫入及執行) 權限，而任何其他使用者 (群組或其他) 則沒有任何權限。

11.2.2.4 在受管理系統上安裝 ELMC Tru64 Unix 軟體套件

首先，解壓縮 ELMC 軟體套件，然後進行安裝。

11.2.2.4.1 解壓縮 ELMC 軟體套件

若要解壓縮 ELMC 安裝套件，請將套件 .gz 檔案放置於暫存目錄中，然後解壓縮：

```
# gunzip WEBES{version}.tar.gz
```

接著，解壓縮檔案。如果當您執行此指令時已經有「套件」子目錄，請確定在此子目錄中沒有先前的 WEBES 套件檔案之後，再執行這個指令。

```
# tar -xvf ELMC_{version}.tar
```

這個指令會建立套件目錄 (如果該目錄尚未存在)，並解壓縮 ELMC 安裝檔案。

11.2.2.4.2 安裝 ELMC 軟體套件



附註： 如果您正在 TruCluster 環境中進行安裝，請先確定所有的節點都已啓動且正在執行之後，再繼續執行。

當您目前所在的目錄是解壓縮套件的目錄時，請輸入下列指令，以安裝適用於 ELMC WCCProxy 的檔案。

```
# setld -l kit
```

請勿執行 setld -D 將 ELMC 安裝指向非預設的目錄。預設目錄對於適當的 ELMC 作業而言是必要的。

套件會開始安裝並完成，不會提示使用者。當您返回 shell 提示 (#) 時，便代表安裝已完成，而 wccproxy 程序會在執行中。

11.3 在 WEBES 使用者介面中更新 ELMC 通訊協定

因爲 WEBES 會自動安裝在 CMS 上，之後 ELMC 儲存庫套件才能分送並安裝在受管理系統上，所以您需要登入 CMS 上的 WEBES 介面並修改通訊協定來包含 ELMC。請在您的 CMS 上完成下列步驟：

1. 開啓 System Event Analyzer 介面：

   開始 → **程式集** → **Hewlett-Packard Service Tools** → **Service Event Analyzer** → **Service Event Analyzer**

2. 在畫面頂端的工具列上，按一下 **Configure Webes Managed Entities** 圖示。

3. 從清單中選擇您的受管理系統，然後按一下主機名稱連結。
4. 在 Managed Entity Properties 畫面上，從下拉式功能表中選擇啓用 ELMC。

Managed Entity Properties

Setting	Value
User-Definable Entity Name	.hp.com
Entity Name on the Network	.hp.com
System Type	ManagedSystem
System Subtype	ProLiant
ELMC	off disabled off DefaultELMC defaultCommandView
SNMP	
WBEM	
Warranty Check	Check
Entitlement type	Warranty
Entitlement Serial Number	USI
Entitlement Product Number	3
Entitlement ID	
Obligation ID *Customers in North and Latin America with Compaq Contract ID or HP CarePack entitlement should enter their Compaq Software Obligation ID (if any) as well:*	
Custom Delivery ID	
Physical Location	

5. 套用變更並關閉 System Event Analyzer。

12 HP Insight Remote Support Advanced 的 EVA 支援需求

12.1 瞭解不同的伺服器類型和軟體應用程式

需要一部或多部 Windows ProLiant 伺服器來裝載您環境中必要的 Remote Support 和 EVA 監視軟體應用程式；實際的裝置數目取決於用來支援 EVA 的 CommandView 版本。

- Insight Remote Support Advanced 和 HP Systems Insight Manager (HP SIM) 一定需要中央管理伺服器 (CMS)，不過，CMS 上可以同時裝載 CommandView 8.0.1 和更高版本，因此不需要另外使用 SMS。
- 所有版本的 CommandView 8.0 及更早版本都需要個別的儲存管理伺服器 (SMS)。



警告！ CommandView 8.0 及更早版本不能裝載於 CMS 上，而對於那些 CommandView 版本，則需要個別的 SMS 或 SMA 及個別的 CMS。CommandView 8.0 是安裝 CommandView 8.0.1 時必須安裝的必要元件。在 CMS 上，請勿安裝舊版的 StorageWorks CommandView EVA。「請勿」在 SMS (執行 CommandView 8.0 或更早版本的系統) 上安裝 WEBES、HP SIM 或 Insight Remote Support Advanced Client。

12.1.1 中央管理伺服器 (CMS)

HP Insight Remote Support Advanced 是 HP Systems Insight Manager (HP SIM) 的外掛程式。Insight Remote Support Advanced 與 HP SIM 軟體應用程式都裝載於中央管理伺服器 (CMS) 上，而且需要其他軟體元件，才能管理客戶環境並提交設定集合和事件資料給 HP 支援中心，以進行分析和回應。

《`HP Insight Remote Support Advanced CMS Configuration and Usage Guide`》中定義的基本 CMS 設定是必要的。符合 CMS 系統使用前提之後，請根據《HP Insight Remote Support Advanced A.05.40 Configuration and Usage Guide》來登錄並設定 CMS。您可以從下列 URL 取得 Insight Remote Support Advanced 技術文件：http://docs.hp.com/en/netsys.html#Remote%20Support%20Pack

12.1.2 儲存管理伺服器

CommandView V8.0.1 也可以安裝在 CMS 上，而不是個別的 SMS 或 SMA 上。不過，只有儲存管理伺服器 (SMS) 或儲存管理設備 (SMA) 才支援所有舊版的 CommandView。CommandView EVA 會將事件寫入至 SMS/SMA 上的 Windows 應用程式記錄檔。SMA 實際上就是 Windows 2000 平台上的 SMS。

為了簡單起見，除非有必要強調這兩種儲存管理類型之間的差異，否則本文一律以 SMS 表示。

本章其餘部分根據您選擇使用的機型而分為較大的幾個小節：

- 「CMS 上裝載的 CommandView 8.0.1 和更高版本」
- 「獨立 SMS/SMA 上裝載的 CommandView」
- 「在 ABM 上使用 CommandView 來支援 EVA4400 的需求」
- 「疑難排解 EVA 受管理系統」

12.2 CMS 上裝載的 CommandView 8.0.1 和更高版本

如果您選擇在中央管理伺服器 (CMS) 上裝載 CommandView 8.0.1 軟體，請閱讀本節。如果您想要將目前的 CommandView 軟體裝載於個別的 SMS 伺服器上，或是想要使用 CommandView 8.0 或更早的版本，則必須將 CommandView 安裝在該個別的 SMS 裝置上，且應該跳至「獨立 SMS/SMA 上裝載的 CommandView」。



重要： 下列內容節錄自 HP StorageWorks CommandView EVA 和 HP Systems Insight Manager 安裝指示。若要在相同的伺服器上安裝 HP CommandView EVA 8.0.1 和 HP Systems Insight Manager 5.3.1，請依照下列指示執行。

在執行這些安裝程序之前，請確定符合下列管理伺服器需求：

- 已安裝支援的 Microsoft Windows 版本。
- 先前未安裝 HP CommandView EVA。
- 已安裝 Windows 的 SP2 安全性修補程式。

12.2.1 重要的連接埠設定資訊

WBEM / WMI 和 SMI-S 的預設連接埠指派 5989 已造成與 CMS 上的 HP-SIM 發生衝突。WEBES 子元件與 WBEM 指示的互動能力、WMI Mapper 及將 HP-UX 系統納入環境中，會使得設定環境變得更複雜。HP-UX 是設定為使用連接埠 5989。下列各節描述的變更可以解決連接埠指派問題，這些變更也會提供新的解決方案，用於透過 CommandView SMI-S 設定 Insight Remote Support Advanced。



附註： 如果您已經完成設定 Insight Remote Support Advanced 環境，而且也可以正常運作，則您可以選擇不做任何改變，而且只有在發現相關的問題時再準備採取下列步驟。

在 CMS 上安裝 HP SIM 和 CommandView SMI-S 的順序會影響預設連接埠設定。目前的最佳作法是建議先安裝 `HP SIM`，並允許 WMI Mapper 使用預設的連接埠 5989。CommandView 安裝會偵測此連接埠是否在使用中，並重新導向至不同的連接埠。

請從指令視窗中執行下列指令，以評估環境中目前的連接埠指派：

```
C:\ netstat -anb >netstat.txt
```

12.2.2 關於新 HP SIM 安裝的重要資訊

如先前所述，最佳作法是在安裝 CommandView EVA 之前先安裝 HP SIM。本節及其小節僅適用於 CMS 上「全新」的 HP SIM 安裝。

1. 在安裝 HP SIM 期間，First Time Wizard 會提示您設定 WBEM / WMI Mapper Proxy。

   圖 12-1 HP SIM First Time Wizard

   將預設值保持為連接埠 5989。完成 HP SIM 安裝之後，將 CommandView SMI-S 要使用的連接埠新增至下列步驟的範例中所示的 xml 檔。

2. 識別 HP SIM 將用來連接至 SMI-S 的連接埠。下列範例將連接埠 60000 用於 **namespace interop** 的 SMI-S https 連線。
3. 在文字編輯器中開啟下列檔案：

   ```
   C:\Program Files\HP\Systems Insight Manager\config\identification\
   wbemportlist.xml
   ```

4. 將下列文字行新增至檔案結尾處。



附註： 範例中顯示完整的檔案，紅色的行代表您在檔案中新增的行。

圖 12-2 XML 檔案範例

```
<?xml version="1.0" encoding="UTF-8"?>
<wbemportlist>
  <port id="5989" protocol="https">
    <cimnamespacelist>
      <cimnamespace name="root/cimv2"/>
      <cimnamespace name="vmware/esxv2"/>
      <cimnamespace name="root/hpq"/>
    </cimnamespacelist>
    <interopnamespacelist>
      <interopnamespace name="root/pg_interop"/>
      <interopnamespace name="root"/>
      <interopnamespace name="root/emulex"/>
      <interopnamespace name="root/qlogic"/>
      <interopnamespace name="root/ibm"/>
      <interopnamespace name="root/emc"/>
      <interopnamespace name="root/smis/current"/>
      <interopnamespace name="root/hitachi/dm51"/>
      <interopnamespace name="interop"/>
      <interopnamespace name="root/interop"/>
      <interopnamespace name="root/switch"/>
      <interopnamespace name="root/cimv2"/>
    </interopnamespacelist>
  </port>
  <port id="60000" protocol="https">
    <interopnamespacelist>
      <interopnamespace name="interop"/>
    </interopnamespacelist>
  </port>
</wbemportlist>
```

5. 儲存 `wbemportlist.xml` 檔案。
6. 重新啓動 HP SIM 服務。

   用滑鼠右鍵按一下 Windows Services API 中的 HP Systems Insight Manager 服務，然後從下拉式功能表中選取 **restart**。

12.2.3 連接現有的 HP SIM 安裝



重要： 如果是第一次安裝 HP SIM，請不要執行下列步驟。只有當您已安裝 HP SIM 且已將 WMI Mapper 連接埠重新設定爲預設連接埠 5989 以外的設定時，才適合使用這些步驟。

EVA 的舊版 Insight Remote Support Advanced 受管理系統文件中以 6989 爲範例，說明如何變更 WMI 對應程式的連接埠設定。只有當已安裝 HP SIM 且 WMI Mapper 連接埠已變更爲預設值 5989 以外的設定時，才適合執行下列更正步驟。

執行下列步驟，將 WMI Mapper 連接埠還原爲預設連接埠。



附註： 重新啓動服務之後，在檔案 `cimserver_planned.conf` 中所做的變更會移至名稱爲 `cimserver_current.conf` 的檔案中。

1. 使用 Windows Services API 來停止 Pegasus WMI Mapper Service。

   1. 選取 **[開始]** 和 **[執行]**，在執行欄位中輸入 **services.msc**。
   2. 按一下 **[確定]**。
2. 在文字編輯器中開啓檔案：`C:\Program Files\The Open Group\WMI Mapper\cimserver_planned.conf`
3. 將參考 `httpsPort=6989` 的行中的連接埠號碼變更爲值 `5989`。



附註： 連接埠號碼可能已設爲不同的值，而不是範例中顯示的 6989。

4. 儲存檔案。
5. 重新啓動 Pegasus WMI Mapper Service。
6. 執行 netstat 指令並確認已套用變更。

```
C:\ netstat -anb >netstat.txt
```

以下是 `cimserver_planned.conf` 檔案中文字的範例。

圖 12-3 cimservr 文字範例

```
enableRemotePrivilegedUserAccess=true
enableHttpsConnection=true
enableHttpConnection=false
sslCertificateFilePath=C:\hp\sslshare\cert.pem
sslKeyFilePath=C:\hp\sslshare\file.pem
httpsPort=5989
```

12.2.4 在 CMS 的 HP SIM 使用者介面中變更 WMI Mapper Proxy 連接埠

1. 以系統管理權限存取 HP SIM 使用者介面。
2. 確認 CMS 的現有認證正確無誤：
   a. 存取 **All Systems List**，從清單中選取做爲 HP SIM CMS 的裝置。
   b. 按一下 **Tools & Links** 標籤。
   c. 按一下 **System Credentials** 連結。
   d. 確認登入認證存在且對 CMS 而言正確 (偏好的)，或者，如果有 `Advanced` WBEM 設定，則請確認已針對 SMI-S 使用的連接埠正確設定 WBEM 通訊協定設定，且已提供正確的使用者名稱/密碼認證。
3. 從上方導覽列中，選取 **Options - Protocol Settings - WMI Mapper Proxy**。
4. 選取 localhost 上執行之 WMI Mapper 的 CMS 執行個體圓鈕。
5. 按一下 **Edit** 按鈕。
6. 在 **port number** 欄位中輸入 **5989**。
7. 按一下 **OK**，儲存您的設定。

12.2.5 將預設值還原至 wbemportlist.xml 檔案

1. 在文字編輯器中開啓檔案：`C:\Program Files\HP\Systems Insight Manager\config\identification\wbemportlist.xml`

   以下是先前如何修改文字的範例 (紅色文字)。在您的檔案中，請移除這些文字。

圖 12-4 wbemportlist 檔案範例

```
<!-- WMI Mapper httpsPort=6989  -->
    <port id="6989" protocol="https">
        <cimnamespacelist>
            <cimnamespace name="root/cimv2"/>
        </cimnamespacelist>
   </port>
```

2. 將下列文字行新增至檔案結尾處。



附註： 範例中顯示完整的檔案，紅色的行代表您在檔案中新增的行。

圖 12-5 XML 檔案範例

```
<?xml version="1.0" encoding="UTF-8"?>
<wbemportlist>
  <port id="5989" protocol="https">
    <cimnamespacelist>
      <cimnamespace name="root/cimv2"/>
      <cimnamespace name="vmware/esxv2"/>
      <cimnamespace name="root/hpq"/>
    </cimnamespacelist>
    <interopnamespacelist>
      <interopnamespace name="root/pg_interop"/>
      <interopnamespace name="root"/>
      <interopnamespace name="root/emulex"/>
      <interopnamespace name="root/qlogic"/>
      <interopnamespace name="root/ibm"/>
      <interopnamespace name="root/emc"/>
      <interopnamespace name="root/smis/current"/>
      <interopnamespace name="root/hitachi/dm51"/>
      <interopnamespace name="interop"/>
      <interopnamespace name="root/interop"/>
      <interopnamespace name="root/switch"/>
      <interopnamespace name="root/cimv2"/>
    </interopnamespacelist>
  </port>
  <port id="60000" protocol="https">
    <interopnamespacelist>
      <interopnamespace name="interop"/>
    </interopnamespacelist>
  </port>
</wbemportlist>
```

3. 儲存檔案。
4. 重新啓動 HP SIM 服務。
   - 選取 **Options - Identify Systems**，重新識別 HP SIM 中的所有 WBEM/WMI 系統來更正連接埠參照

12.2.6 安裝和設定 CommandView AFTER HP SIM

CommandView EVA 安裝套件包含 SMI-S 元件。僅限於安裝時，SMI-S 會指派兩個連接埠。SMI-S 會指派的預設連接埠如下 (如果可用的話)：

- http 連接埠=5988

- https 連接埠=5989

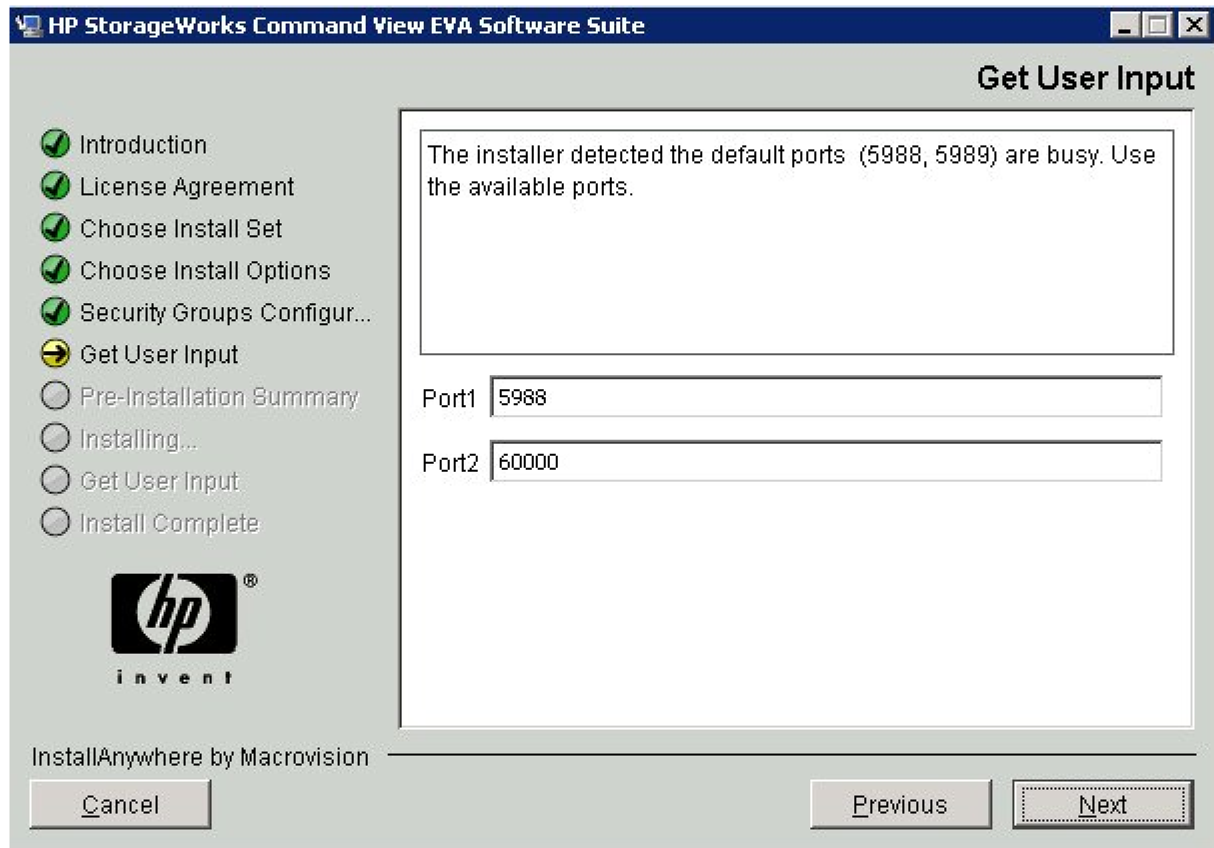
如果其中一個連接埠在使用中或兩個都在使用中，安裝會提供另一個設定畫面，供您變更連接埠號碼。SMI-S 安裝程式會建議使用連接埠 60000 (如果不在使用中的話)。SMI-S 會保留連接埠 5988 (如果沒有衝突的話)。當 HP StorageWorks CIM Object Manager 程序啟動時，SMI-S 會使用這些連接埠。



附註： 只有在偵測到連接埠衝突時才會顯示此畫面。這就是為何強烈建議在安裝 CommandView 之前先安裝 HP SIM 的原因。

下圖是在已使用 WMI Mapper 安裝 HP SIM 的 Insight Remote Support Advanced CMS 上安裝 SMI-S 的範例：

圖 12-6 SMI-S 安裝補充畫面



如需連接埠設定的詳細資訊及設定 CommandView 存取之 Windows 帳戶的相關資訊，請參閱 HP StorageWorks CommandView EVA 安裝指南。HP SIM 和 WEBES 需要這些認證。

使用 `netstat` 指令來驗證這些連接埠之後，

```
C:\ netstat -anb >netstat.txt
```

您會看到下列輸出：

圖 12-7 netstat 結果

```
TCP    0.0.0.0:5988     0.0.0.0:0     LISTENING    1712  [JavaWrapper.exe]
TCP    0.0.0.0:5989     0.0.0.0:0     LISTENING    460   [WMIServer.exe]

TCP    0.0.0.0:60000    0.0.0.0:0     LISTENING    1712  [JavaWrapper.exe]
```



附註： 在上述範例中，SMI-S 是設定爲使用連接埠 5988 和 60000。

12.2.7 當 CommandView 比 HP SIM 先安裝時，請重設連接埠號碼

1. 編輯檔案：

   `C:\Program Files\Hewlett-Packard\SMI-S\CXWSCimom\config\cxws.properties`

2. 找出 `cxws.http.port and cxws.https.port` 項目並重設爲下列值：

   `cxws.http.port=5988`

   `cxws.https.port=60000`

3. 重新啓動 HP StorageWorks CIM Object Manager



附註： 任何需要透過此 SMI-S 對陣列進行通訊的 API，也都需要更新目標連接埠。在獨立的 SMS 設定中，只要 SMS 上沒有其他連接埠發生衝突，CommandView 就應該使用預設連接埠 5988 和 5989 以搭配 Insight Remote Support Advanced 一起運作。

12.3 獨立 SMS/SMA 上裝載的 CommandView

在 CMS 之外另外設定 SMS 時，請以本節及其小節做爲準則。

下列軟體應用程式裝載於 SMS 上，且與 (Insight Remote Support Advanced) 解決方案有關或屬於其中一部分：

- CommandView
- Event Log Monitoring Collector (ELMC)，之前稱爲 WCC Proxy
- MC3 元件



附註： SMS 和 SMA 上的資料夾路徑不同。具體的路徑差異不屬於本文的討論範圍。在此提出是爲了讓您瞭解 CommandView EVA 檔案在 SMA 上是位於不同的資料夾。

從 CommandView V8.0 開始，**新增/移除程式**視窗中已看不到軟體元件 HP StorageWorks SMI-S CIMOM 和 HP StorageWorks SMI-S EVA。請檢查是否有名稱爲 HP StorageWorks CIM Object Manager 的服務及其狀態，以驗證元件是否已安裝且正在執行。請確認 SMS/SMA 已安裝 CommandView EVA 7.0.1 或更高版本，並驗證 SMI-S EVA 和 SMI-S CIM 元件 (也就是構成 SMI-S 的兩個元件)。移至 SMS 上的 Windows 控制台，確定 [新增/移除程式] 對話方塊中有列出下列元件：

- HP StorageWorks CommandView EVA
- HP StorageWorks SMI-S CIMOM
- HP StorageWorks SMI-S EVA

小心： 從主機系統中移除 SMI-s 也會強制移除 Command View Tape Library (CV TL)。CV TL 的版本必須符合磁帶櫃中使用的韌體。

如果 CV TL 所安裝的 SMI-s 版本比 CommandView 使用的版本更舊，請在 CV TL 之後安裝或升級 CommandView，以避免發生衝突。

此外，每一個軟體應用程式使用的認證都會在安裝時被彼此覆寫。因此，建議使用相同的帳戶詳細資料，以避免遺失資訊。



附註： CommandView EVA STANDARD 安裝是取得 Insight Remote Support Advanced 支援的優先條件。



如果沒有安裝必要的 CommandView 元件，如需詳細資訊，請參閱「在 SMS 上設定 CommandView for EVA 的需求和文件」



附註： 您可以在《HP StorageWorks EVA Software Compatibility Reference》中找到 SMS 系統和硬體需求，網址為：

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01525950/c01525950.pdf?jumpid=reg_R1002_USEN (請參閱 PDF 中下列兩個表格；《表 4.1 管理伺服器類型支援的軟體》和《表 4.2 支援的 EVA 軟體作業系統》)。

如需詳細資訊，請瀏覽《HP StorageWorks CommandView EVA Software Suite QuickSpec Overview》，網址為：http://h18004.www1.hp.com/products/quickspecs/12239_div/12239_div.html

12.3.1 在 SMS 上設定 CommandView for EVA 的需求和文件

您可以透過下列 URL 取得 CommandView for EVA 文件：http://h18006.www1.hp.com/products/storage/software/cmdvieweva/index.html (按一下 **Support for your product** 連結，以檢視 CommandView EVA 手冊清單)

進行 CommandView 安裝和設定需要下列文件：

- 《HP StorageWorks CommandView EVA Installation Guide》
- 《HP StorageWorks CommandView EVA 版本號碼 版本注意事項》
- 《HP StorageWorks EVA Software Compatibility Reference》

12.3.2 CommandView 7.0.1 至 8.0.1 with SMI-S 需求概觀

本文適用於 CommandView EVA 7.0.1 至 8.0.1。請務必查閱 CommandView EVA 文件，以瞭解基本的需求。同樣地，CommandView 8.0 版和更早的版本無法在 CMS 上執行。從 CommandView 8.0.1 版發行開始，現在支援在 CMS 上執行 CommandView。基於容錯或負載平衡的目的，一個環境中可以有多個 SMS。但是，不論在任何時候，都只能有一個 CommandView 伺服器在主動管理給定的 EVA 陣列。

若要成為有效的 SMS，伺服器必須安裝 CommandView EVA (7.0.1 版或以上的版本)，且至少要管理一個陣列。SMI-S 隨著 CommandView EVA 安裝一起提供且為必要的，因為它是 HP SIM 與陣列之間的通訊路徑 (使用 CIMOM 進行 WBEM 通訊)。



附註： EVA 的事件資料只會傳遞至主動管理陣列的 CommandView。不過，在任何執行 CommandView 的伺服器上，只要是能夠成為 EVA 裝置陣列的主動管理者，您就應該安裝 ELMC。目前未主動管理 EVA 的任何 CommandView 執行個體，都稱為被動的 CommandView 執行個體。

12.3.3 SMS 或 SMA 系統和存取需求

儲存管理伺服器 (SMS) 存取需求：

- Microsoft Windows 帳戶必須具有正確的群組權限，才能存取 CommandView EVA。

安裝 CommandView for EVA 會在系統中新增兩個新的群組權限，也就是 HP Storage Admins (寫入權) 和 HP Storage Users (讀取權)。

12.3.4 WEBES – EVA 通訊

CMS 上的 WEBES 需要由至少具有讀取權的帳戶提供認證。此使用者名稱和密碼是在 SMS 的 WEBES Managed Entity 頁面中輸入。這樣可讓 WEBES 與陣列進行通訊。如需此程序的詳細資訊，請參閱「CommandView EVA 密碼設定」。

12.3.5 HP SIM – EVA 通訊

SMI-S 可讓 HP SIM 與 EVA 陣列之間使用 WBEM 通訊協定進行通訊。CommandView 8.0 版之前版本隨附的 SMI-S 採用 CIMOM，具有獨立的使用者認證，定義來允許使用此 WBEM 通訊路

徑。從 CommandView 8.0 版和以上版本開始，SMI-S 已建立憑證信任且使用 CommandView 認證 (如「SMS 或 SMA 系統和存取需求」所述)。

在 CommandView 8.0 版之前，安裝 CommandView EVA 會在 SMS 上建立帳戶的 cimuser 認證，使用者名稱為 administrator，密碼為 administrator。SMS 上必須先存在權限等級至少為讀取權的 Windows 系統管理員帳戶 (例如，「SMS 或 SMA 系統和存取需求」中所述的 HP Storage Users)，才能順利地自動建立此 cimuser 身分。



重要： HP SIM 要求 System Protocol Settings 頁面中必須輸入這一組使用者認證 (請參閱「HP SIM 中關於 WEBES 的設定」)，SMS CIMOM 才能與 EVA 之間傳遞 WBEM 通訊。

在 CommandView 8.x 版中，這種情形已改變。SMI-S 已沒有獨立的使用者名稱/密碼。現在使用 CommandView 和 SMI-S 之間的信任關係，採取單一登入 (SSO) 設計。CommandView 使用者名稱和密碼用於 SMI-S 連線。

CommandView for EVA 文件包含設定自訂系統管理員帳戶的其他資訊。在設定 WBEM 認證之後，如果您無法讓 HP SIM 找到 EVA 陣列，或是如果不確定密碼設定，請至「疑難排解 SMI-S 認證」，其中會說明如何修改或重設這些認證。另請參閱「疑難排解 WBEMDISCO」，其中說明 WBEMDISCO 公用程式的用法，此公用程式可用來測試使用者名稱和密碼。



附註： 可能有其他應用程式使用 HP SIM 做為連接 EVA 的介面 (例如 Storage Essentials)。如果這類應用程式執行主動的管理功能，則可能需要寫入權。在此情況下，您應該確定 cimuser 帳戶與具有 HP Storage Admins 群組權限的 Windows 帳戶相關聯。

12.3.6 SMS 上需要的軟體

SMS 上需要有下列軟體應用程式，SMS 和 EVA 才能使用 Insight Remote Support Advanced 支援：

- 支援的 HP StorageWorks CommandView EVA 版本，其中包括 SMI-S (為 EVA Remote Support 所必備)。
- CommandView for EVA 套件預設會安裝 SMI-S。SMI-S 由兩個元件組成 (SMI-S CIMOM 和 SMI-S EVA)，而 SMS 上需要這兩個元件。



重要： 雖然 SMI-S 在 CommandView 安裝中為選擇元件 (但根據預設，在標準安裝會納入)，但在 SMS 上是取得 EVA 裝置遠端支援所「必要的」，如果您選擇執行 CommandView EVA「自訂」安裝，請勿取消選取 SMI-S。



警告！ 如果 SMS 已安裝多個版本的 CommandView EVA，可能遺留一些檔案及 (或) 登錄項目，而這些項目不利於 SMI-S 的運作。如需詳細資訊，請參閱下列建議：《`HP StorageWorks CommandView EVA v6.x to v7.0 Upgrade Issue with the v5.0.3 Patch Installed`》.

- Windows ELMC (又稱為 WCCProxy)「只會」下載到要在 SMS 上為了支援 EVA 裝置而安裝的 CMS。
- HP SIM 和 Insight Remote Support Advanced 需要 ProLiant Insight Management Agents，才能將 SMS 識別為受管理系統。HP SIM 支援 IM Agent 6.30 版或以上版本，但除非 SMS 是 SMA，否則建議您升級至最新可用的版本。



警告！ 如果您的儲存管理裝置是 SMA，則「不建議」升級至最新版的 ProLiant Management Agents，因為只有特定版本的 Insight Management Agents 在 SMA 上才有效。HP SIM 和 Insight Remote Support Advanced 也需要 SNMP 服務，才能支援 SMS 做為受管理系統。

- HP SIM 和 Insight Remote Support Advanced 也需要 SNMP 服務，才能支援 SMS 做為受管理系統。

12.3.7 滿足 Windows SMS 的 ELMC 一般需求

除了上述列出的SMS需求之外，受管理系統(SMS)還必須符合下列基本需求，才能安裝ELMC。

磁碟空間：在安裝時，已安裝 Windows 作業系統的磁碟機上總共必須有 40MB 的可用空間 (%SystemDrive%，根據預設，通常是 C:)。安裝完成之後總共會使用 30MB 的空間。

12.3.7.1 安裝條件和需求

ELMC 軟體的位置：從 RSSWM 下載至 CMS 的 ELMC for Windows 元件必須複製到受管理系統上的本機磁碟機。如果您對應至屬於另一個系統的磁碟機代號，安裝將會產生錯誤。



重要： 必須從 SMS 的「本機」磁碟機執行 ELMC 安裝，不支援從遠端對應共用執行安裝。

12.3.7.2 必要的權限和存取權

若要安裝、移除或更新 ELMC，使用者 ID 必須為下列其中一個：

- 電腦上 Administrators 群組的成員
- 某個群組的成員，而此群組又是電腦上 Administrators 群組的成員。例如，如果使用者 ID 是 Domain Admin，且您已將 Domain Admins 新增至本機電腦上的 Administrator 群組，則您已具有必要的權限。若要將 Domain Administrators 新增至本機 Administrator 群組，請依照您的作業系統來採取適合的程序。

ELMC提供通訊路徑讓WEBES監視CommandView所寫入的事件資料。建立此通訊路徑之後，WEBES 會分析在 Windows 應用程式事件記錄檔中找到的事件資料。如果尚未建立應用程式事件記錄檔，則這項初次分析可能會花費很久的時間才完成，且會消耗SMS和CMS兩者的頻寬。此外，在完成初次清除之前，無法傳遞安裝結束時所傳送的 SEA 測試事件及任何新的事件。

最佳作法是在安裝之前封存舊的事件資料並清除應用程式事件記錄檔，以降低此額外負荷。WEBES 建議將應用程式事件記錄檔內容大小設為至少 10MB 及「視需要而定」覆寫時間。可能需要根據環境來調整這些設定。如需詳細資訊，請參閱「清除 SMS 上的事件記錄檔」。

12.3.7.3 設定 SNMP 服務

您必須在 SNMP Server Properties 中設定 CMS 的社群和 IP 位址，以便 ProLiant SMS 能夠成為向 CMS 回報的受管理伺服器。若要設定 SNMP 服務，請執行下列步驟：

1. 從服務中，用滑鼠右鍵按一下 **SNMP Service**，然後選取**Properties**。
2. 選取**Security**標籤，輸入 HP SIM 的 HP SIM Global Protocol Settings 頁面中的`Community`名稱。
3. 若要檢查 HP SIM 中定義的社群名稱，請執行下列步驟：
   a. 移至 **Options - Protocol Settings - Global Protocol Settings**。
   b. 在 Global Protocol Settings 頁面的 Default SNMP settings 區域中，檢查 **Read** community string 欄位中的項目。

圖 12-8 Default SNMP settings 區域

4. 選取 **Traps** 標籤。
5. 輸入`Community`名稱。
6. 輸入`Trap`目的地。這是 CMS 的 TCP/IP 位址。localhost 或回送位址也必須納入爲目的地；如果不是，HP-SIM 將無法從 SMS 擷取足夠的資訊，也就無法通過 Remote Support 授權檢查 (RSEC)。
7. 按一下**確定**。

12.3.7.4 在 SMS 上安裝 ELMC 以取得 EVA Remote Support

12.3.7.4.1 準備 SMS 以執行 ELMC 安裝

「唯有」當您在 SMS 上已安裝「任何」版本的 HP ISEE Client、WEBES、OSEM 或 WCCProxy 時，才需要進行這些步驟 (「從 SMS 中移除 HP ISEE」至「從 SMS 中移除 OSEM」)。

12.3.7.4.1.1 從 SMS 中移除 HP ISEE

「唯有」當您在受管理系統上已安裝 HP Instant Support Enterprise Edition (ISEE) 時，才需要進行這些步驟。如果您沒有在受管理系統上安裝 ISEE，可以跳過這一節。



重要： Instant Support Enterprise Edition (ISEE) A.03.95 及舊版與 Insight Remote Support Advanced「不是相同的應用程式」，請不要安裝在任何 SMS 上。

若要移除 ISEE，請執行下列步驟：

1. 在控制台中，連按兩下 **[新增/移除程式]**。
2. 在 **[新增/移除程式]** 對話方塊中，找出 ISEE 項目 (如果有的話)，然後按一下 **[移除]**。

12.3.7.4.1.2 從 SMS 中移除 WEBES



附註： 從 SMS 中移除 ISEE 之後，如果移除 WEBES ，應該也會一併移除 WCCProxy。如果未移除 ISEE，則 WEBES 不會移除 WCCProxy。



秘訣： 在移除 WEBES 之前，建議您存取 System Event Analyzer (SEA) UI，並從 Managed Entities 頁面中找回系統序號和產品 ID。之後當您在 CMS 的 HP SIM 中設定受管理系統的內容時，此資訊就可以派上用場。

若要從 SMS 中解除安裝所有 WEBES 工具 (包括 WCCProxy)，請依照下列步驟執行：

1. 使用具備系統管理員權限的帳戶登入 SMS。
2. 將所有正在執行的工具全部關閉。

3. 在控制台中，連按兩下 **[新增/移除程式]**。
4. 在 **[新增/移除程式]** 對話方塊中，找出 WEBES 項目並按一下 **[變更/移除]**，以執行安裝精靈。
5. 出現提示時，選擇 **Remove** 選項。
6. 依照提示來執行解除安裝。
7. 在 **[新增/移除程式]** 對話方塊中，確認沒有 WCCProxy 項目。如果有這個項目，您可以選取它並按一下 **[移除]**，手動將它移除。

12.3.7.4.1.3 從 SMS 中移除 OSEM

解除安裝將會完全移除 OSEM 目錄下的所有檔案。如有需要，您可以手動備援設定檔案，例如 `working.props`、`hosts.txt` 或 `communities.txt`。

您可能也想要備援通知資料夾，以保留所有問題報告的複本。OSEM 1.3.7 或以上版本在解除安裝過程中會建立所有設定和狀態資訊的複本。

若要從 SMS 中解除安裝所有 OSEM 工具，請依照下列步驟執行：

1. 使用具有系統管理員權限的帳戶登入。
2. 將所有正在執行的工具全部關閉。
3. 在控制台中，連按兩下 **Add/Remove Programs**。
4. 在**新增/移除程式**對話方塊中，找出 OSEM 項目並按一下**移除**，以執行安裝精靈。



小心： 在安裝精靈中，第一個 Cancel 按鈕是您徹底結束解除安裝常式的唯一機會。之後，即使有取消或結束選項可用，也不要再取消或停止解除安裝。

5. 遵循提示繼續解除安裝。

12.3.7.4.2 清除 SMS 上的事件記錄檔

在 EVA Remote Support 情況下，此爲選用步驟，但 HP 建議您在安裝 ELMC 之前，先封存並清除 SMS 上的應用程式記錄檔。

在初次安裝並啓動 ELMC 時，WEBES 會處理最近記錄的事件，而這可能會暫存佔用資源。一般而言，當您在疑似有問題的系統上安裝 ELMC 時，此功能很有用，因爲應用程式記錄檔資訊在解決問題時會非常有用。

在安裝 ELMC 之前，請依照下列步驟來封存和清除 Windows 應用程式事件記錄檔：

1. 開啓事件檢視器：

   在 Windows Server 2003 上：**開始 | 程式集 | 系統管理工具 | Event Viewer**

2. 在事件檢視器視窗的左邊窗格中，按一下應用程式記錄檔。

   清除所有事件：選擇 **Action | Clear all Events**。清除之前，您可以選擇將現有的事件儲存至另一個檔案。儲存的記錄可留待以後進行進一步分析。除非您認爲保留目前的事件清單沒有意義，否則請將記錄儲存至您選擇的目錄。

3. 關閉事件檢視器。

12.3.7.4.3 在 SMS 上安裝 ELMC



附註： 如果您在 CMS 上安裝 CommandView 8.0.1，則 CMS 已要求一個 ELMC 執行個體，您不需要再安裝第二個執行個體。如果您在不是 CMS 的 SMS/SMA 上安裝任何版本的 CommandView，且想要從遠端監視該伺服器，則「需要」這個 ELMC 執行個體。

符合第一章所述的使用前提之後，若要安裝 ELMC 套件，請執行下列步驟：

1. 從 CMS 中將 ELMC 安裝執行檔下載到 SMS。

   安裝執行檔位於 CMS 的下列資料夾：

   - `%system driver%\Hewlett-Packard\Business Support\ELMC\Windows_x86_x64`

安裝程式檔的檔案名稱與下列檔案名稱相似：

- `ELMC_WCCProxy_v###_Windows_x86_x64.exe`



附註： Remote Support Software Manager 中的 Windows ELMC 套件是 ProLiant CMS 的可執行檔，「而且」也是可移植到 SMS 的儲存庫。

2. 在 SMS 上，按兩下 `ELMC___.exe` 檔案。

   接著會顯示一連串進度視窗，最後完成安裝。

   不需要使用者輸入任何資料，也不會出現任何提示。

3. 不會出現 ELMC 安裝完成的通知 (未來的 ELMC 版本中會修正這一點)。
4. 若要確認 ELMC 已完成安裝且正在執行，請在 SMS 上開啓指令視窗並執行下列指令：

   `wccproxy status`

   應該會傳回輸出 `The WCCProxy service is running`。

12.3.8 在 CMS 上設定 EVA 特定資訊

12.3.8.1 CommandView EVA 密碼設定

CommandView EVA V6 和以上版本採用安全登入 (SSL) 設計，所以需要有 Windows 帳戶使用者名稱和密碼，才能存取 CommandView EVA 使用者介面，如「SMS 或 SMA 系統和存取需求」中所述。CommandView for EVA UI 使用者名稱和密碼也是 WEBES 與 EVA 陣列進行通訊所必要的，且必須在 WEBES SEA Web 介面的 Managed Entities 畫面中手動輸入，才能處理 EVA 事件。此使用者名稱和密碼沒有預設值。這是由系統管理員設定。帳戶至少需要有讀取權 (`HP Storage Users`) 群組權限。



附註：

- CMS 上的 HP SIM 與 EVA 進行通訊時，是採用 SMS 上的 SMI-S 所提供的 WBEM 通訊協定 CIMOM。
- CMS 上的 WEBES 會與 SMS 上的 ELMC 進行通訊，再轉而使用 SMS 上的 CommandView 與 EVA 進行通訊。

如需設定有效 SMS 和陣列的相關資訊，請參閱 CommandView EVA 安裝文件。您可以透過下列 URL 取得 CommandView for EVA 文件：

- http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01375105/c01375105.pdf?jumpid=reg_R1002_USEN

  (按一下 **Support for your product** 連結，以檢視 CommandView EVA 手冊清單)

  進行 CommandView for EVA 安裝和設定需要下列文件：

  — 《`HP StorageWorks CommandView EVA Installation Guide`》
  — 《`HP StorageWorks CommandView EVA`》
  — 《`HP StorageWorks EVA Software Compatibility Reference`》

12.3.8.2 設定 SMS 與 CMS 之間的信任關係

1. **設定 SMS 與 CMS 之間的信任關係：**



附註： 此信任關係可讓 CMS 上重新顯示 HP SIM 至 CommandView EVA 陣列頁面的連結。

設定這種信任關係並不是必要條件。不過，卻可讓 SIM 從 CommandView 收集大量額外的資訊，並在 HP-SIM 內的 SMS 頁面上透過連結來提供這些資訊。

   a. 使用 CommandView UI，選取頁面右上角的 **Server Options** 連結。這時會開啓 Management Server Options 頁面。

b. 選取 **System Insight Manager/Replication Solutions Manager trust relationships** 按鈕。這時會開啓 SIM/RSM Trust Relationship 頁面。
c. 選取 **Install Certificate** 按鈕。輸入 CMS 的 DNS 位址。
d. 選取 **Install Certificate**。

2. **確認已載入 SMI-S 的憑證：**
a. 使用 CommandView UI，選取頁面右上角的 **Server Options** 連結。這時會開啓 Management Server Options 頁面。
b. 選取 **Other Application Trust Relationships** 的按鈕。
c. 確認已載入本機 SMS 的 `SMI_EVA_Provider` 憑證。

如果遺失 SMI_EVA_Provider 憑證，請參閱「SMA 上的 CommandView SSO 憑證：將 SSO 憑證新增至 CommandView EVA truststore 信任庫 」，其中提供載入此憑證的指示。

12.3.8.3 HP SIM 中關於 WEBES 的設定

1. 在 HP SIM 找到執行 CommandView 的伺服器 (正在管理 EVA 陣列) 之後，請在 HP SIM 中設定其系統內容。

在 HP SIM 中設定受管理系統的系統設定，如下所示：

- 您可以在 HP SIM 中設定多個系統的系統設定 (**Options ¦ System Properties ¦ Set System Properties**)。
- 在 HP SIM 中，您可以從 HP SIM 集合中選取系統，或在 HP SIM 中搜尋系統，以設定個別系統的所有設定。當 HP SIM 中顯示伺服器的詳細資訊後，請選取 **Tools and Links** 標籤，再選取 **Edit System Properties** 連結。



附註： 在 SMS (和連接的 EVA 裝置) 的 HP SIM 中，WEBES 會從 System Properties 頁面中擷取受管理實體資訊：

- 公司資訊
- 連絡資訊
- 序號
- 產品 ID
- 合約資訊

您必須提供此資訊，才能確保 SMS 通過 `Remote Support 授權檢查 (RSEC)`，且能夠將事件傳遞至 HP 支援中心。

`EVA-LE 陣列的例外`。WEBES 會直接與 EVA-LE 陣列進行通訊，以取得產品型號和產品序號。如果 HP SIM System Properties 欄位中有此資訊，則會覆寫自動偵測的資訊。

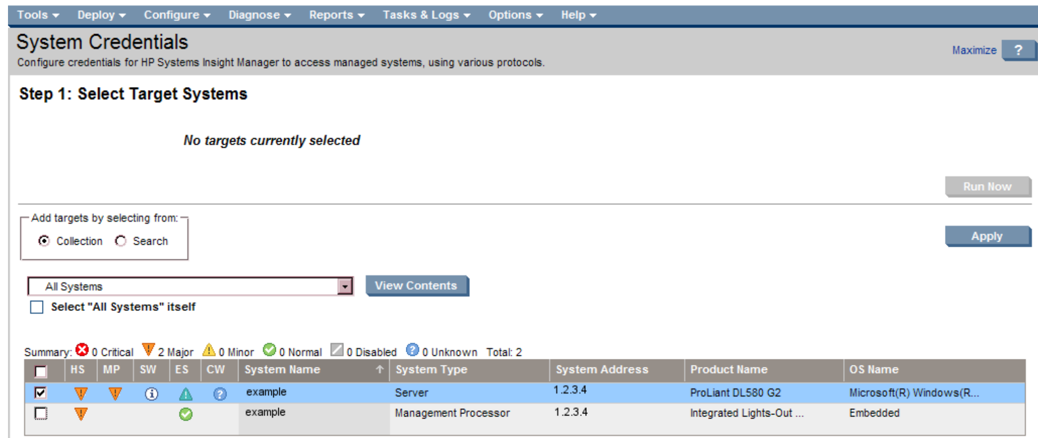
如需設定系統設定的詳細資訊，請參閱《`A.05.40 Insight Remote Support Advanced Configuration and Usage Guid`》，網址為：

http://docs.hp.com/en/netsys.html#Remote%20Support%20Pack

若要在 HP SIM 中設定系統的 WBEM 設定，請執行下列步驟：

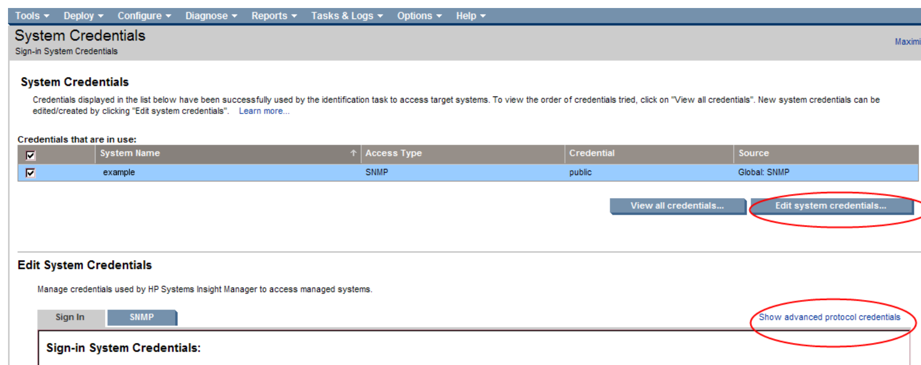
`HP SIM 5.3.1`

a. 選取 **Options > Security > Credentials > System Credentials** 。
b. 在 **Systems Credentials** 畫面搜尋系統，或從 System Type 下拉式清單中選取系統，然後按一下 **Apply**。

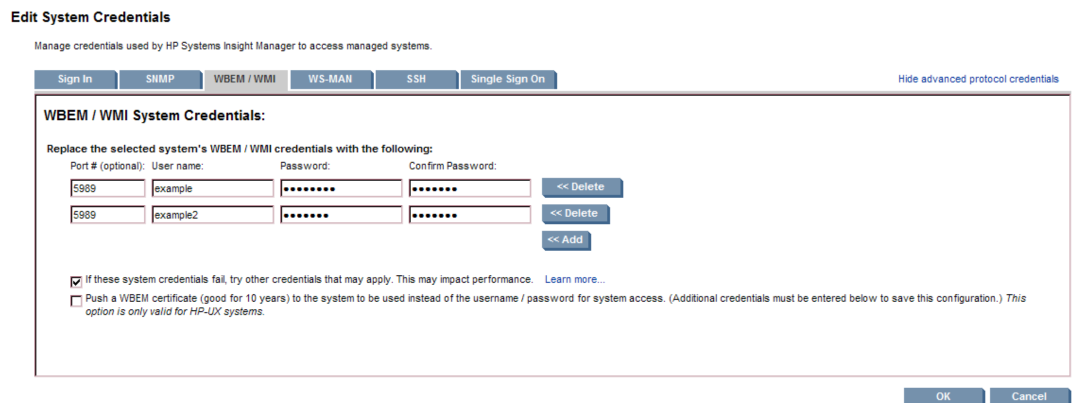


c. 按一下 **Run Now**。

d. 在 **System Credentials** 畫面中按一下 **Edit system credentials** 按鈕，畫面會展開。



e. 在畫面的 **Edit System Credentials** 區段按一下 **WBEM/WMI** 標籤。您現在可以為此受管理系統設定特定的 WBEM/WMI 認證，或者您可以使用在上一個步驟中設定的通用預設。只需驗證 **If these system credentials fail, try other credentials that may apply...** 核取方塊已選取，然後按一下 **OK**。



HP SIM 5.3.1

a. 移至 **Options**¦**Protocol Settings**¦**System Protocol Settings**。

b. 在 `Step 1: Select Target Systems` 頁面中，從下拉式清單中選取 HP SIM 集合 (包含執行 CommandView 的伺服器)，以顯示與該集合相關聯的系統。

c. 從清單中選取您的系統，然後按一下 **Apply**。

d. 再選取系統一次，然後按 **Next**，以顯示 `Step 2: Specify the communications protocol settings for target systems` 頁面。

e. 在 `WBEM settings` 區段中，選取 **Update values for this protocol** 核取方塊，並依需要編輯設定。SMI-S 使用預設連接埠 5989。

圖 12-9 System Protocol Settings 頁面。

System Protocol Settings

Target:

WBEM settings

Update values for this protocol

Use global defaults (Port #:); (User name:administrator)

Use values specified below (either fill in *User name* and *Password* fields, or select corresponding *Use certificate instead* checkbox)

	Port #:	User name:	Password:	Confirm password:	Use certificate instead
1.		administrator	••••••••••••••••••	••••••••••••••••••	
2.					
3.					
4.					
5.					



附註： 在 HP SIM 中，也可以透過 **Options ¦ Protocol Settings ¦ Global Protocol Settings** 來設定全域通訊協定設定。

f. 按一下 **Run Now**，套用您所做的變更。

2. 對 SMS 再執行一次「探索」會產生 HP SIM System 清單中列出的 EVA。

如果 EVA 陣列沒有出現，則表示 HP SIM 與 SMI S 之間的通訊有問題，請參閱「HP SIM 未探索 EVA」。

12.3.8.4 設定 WEBES

12.3.8.4.1 提供 WEBES 中的 SMS 受管理系統實體資訊

WEBES 會從 HP SIM 擷取所有必要的受管理實體資訊，但不包括 CommandView 使用者認證。識別爲「CommandView 伺服器」的受管理實體是指識別爲 SMS 的系統。



附註： 如果 WEBES 中的 Managed Entities 頁面將 SMS 識別為 CommandView 伺服器以外的項目，請確認 SMS 上是否已安裝 ELMC，然後重新啟動 DESTA，如下所示：

1. 開啟指令提示字元並執行下列指令：net stop desta_service
2. 使用下列指令重新啟動 DESTA：net start desta_service
3. 如果重新啟動 DESTA 也無法解決問題，請從 WEBES 的 Managed Entities 頁面中移除伺服器，然後再重新啟動 DESTA 一次。
4. 在 Managed Entities 頁面中選取每一個 SMS 的 CommandView 通訊協定。這是用來登入 CommandView EVA 的 Windows 帳戶使用者名稱和密碼：
   a. 開啟 System Event Analyzer 介面：

      開始 --> 程式集 --> Hewlett-Packard Service Tools --> Service Event Analyzer --> Service Event Analyzer

   b. 在畫面頂端的工具列上，按一下 **Configure Webes Managed Entities** 圖示。



   c. 從清單中選擇您的受管理系統，然後按一下主機名稱連結。
   d. 在 Managed Entity Properties 畫面上，從下拉式功能表中選擇啟用 CommandView 通訊協定。

Managed Entity Properties

Setting	Value
User-Definable Entity Name	example.example.com
Entity Name on the Network	example.example.com
System Type	ManagedSystem
System Subtype	ProLiant
ELMC	off (disabled / off / DefaultELMC / defaultCommandView)
SNMP	
WBEM	
Warranty Check	Check
Entitlement type	Warranty
Entitlement Serial Number	USE5
Entitlement Product Number	371293-405
Entitlement ID	
Obligation ID *Customers in North and Latin America with Compaq Contract ID or HP CarePack entitlement should enter their Compaq Software Obligation ID (if any) as well:*	
Custom Delivery ID	
Physical Location	
* Choose a Site	no site / Refresh List / Go To Sites

   e. 套用變更並關閉 System Event Analyzer。

12.3.8.4.2 測試從 SMS 傳送事件

若要測試從 SMS 傳送事件至 CMS，請執行下列步驟：

1. 在 HP-SIM 中 `Remote Support and Configuration Services` 選項的 **Entitlement** 頁面中，確認 SMS 及其相關聯的 EVA 裝置都已啟用遠端支援。
2. 在 SMS 上開啟指令視窗，並執行指令 `wccproxy status`。應該會傳回輸出 `The WCCProxy service is running`。

3. 執行指令 `wccproxy test`。這會將測試事件寫入至 SMS 上的 Windows 應用程式事件記錄檔。接著，SMS 上的 ELMC (WCCProxy 程序) 應該會在五分鐘之內讀取新的事件，然後將事件資料傳送至 CMS 上的 WEBES。

   CMS 上的 WEBES 接著會分析測試事件，並傳送通知給 CMS 上的 HP SIM 和 Remote Support Client (RSC)。

   如果您已在 Web 瀏覽器中連線至 CMS 上的 WEBES SEA Web 介面，則您在 Web 瀏覽器中也會看到 Problem Report 結果。同樣地，WEBES Problem Report 也應該會出現在 HP SIM Web 介面、RSC 使用者介面及 HP Remote Support 後端系統中 (透過應用程式管理主控台 (AMC) 檢視)。

12.4 在 ABM 上使用 CommandView 來支援 EVA4400 的需求

引進 EVA4400 已在 HSV300 控制器配對中新增一個會在陣列中安裝 CommandView 的模組。這稱為陣列型管理 (Array Based Management，簡稱為 ABM)，具有可透過 LAN 存取的網路介面。ABM 無法在陣列中裝載 SMI-S，所以 SMI-S 必須裝載於 LAN 中的其他位置上，以做為連接陣列的 Proxy 連線。

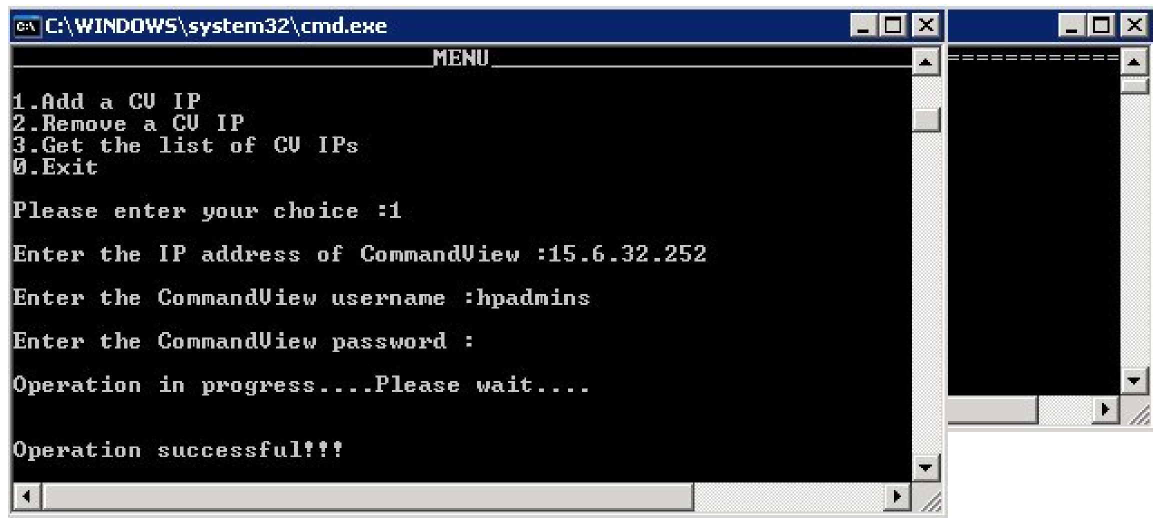
CommandView 安裝套件可以將 SMI-S 獨立安裝在指定的伺服器上。SMI-S 可以安裝在 Insight Remote Support Advanced CMS 或 LAN 中另一部支援的伺服器上。本文稍早所解釋之連接埠衝突的相關程序是針對在 CMS 上設定 SMI-S 的情形，因為 HP SIM 需要透過 SMI-S 指派的連接埠來連線至陣列。

1. SMI-S 包含一個稱為 `discoverer.bat` 的公用程式，可用來設定連接至陣列 ABM 的連線。這可讓 SMI-S 使用目標 ABM 的 IP 位址和認證，將連線要求傳送至陣列。執行下列檔案將會啓動此程序：

   ```
   C:\Program Files\Hewlett-Packard\SMI-S\EVAProvider\bin\
   discoverer.bat
   ```

   這時會開啓指令視窗：

   圖 12-10 SMI-S ABM 設定



附註： 上述範例中的第一行將 `http://localhost:5988` 定義為 SMI-S 的預設路徑。如果在 CMS 上依照「連接埠設定」資訊所述來操作，則可能已變更此 http 連接埠。這是 http 連接埠。第二行和第三行要求必須對 HP Storage Group 存取權所設定的帳戶提供認證。輸入這些項目後，就會顯示功能表。

2. 選取 **1** 來新增 CV IP。
3. 在 ABM 上輸入 CommandView 的 IP 位址和認證。

```
1.Add a CV IP
2.Remove a CV IP
3.Get the list of CV IPs
0.Exit

Please enter your choice :1

Enter the IP address of CommandView :15.6.32.252

Enter the CommandView username :hpadmins

Enter the CommandView password :

Operation in progress....Please wait....

Operation successful!!!
```

4. 選取 **3** 來檢視 CV IP 位址清單。

```
________________________________MENU________________________________
1.Add a CV IP
2.Remove a CV IP
3.Get the list of CV IPs
0.Exit

Please enter your choice :3

__________CommandViews currently discovered by SMIS__________

   1.2.3.4
```



附註： 如果 CommandView 安裝在執行 discoverer 的本機主機上，則您在此清單中也會看到本機主機的 IP 位址。

5. 輸入 **0** 來結束 discoverer 公用程式。

當 SMI-S 連線至 ABM 之後，如果 HP SIM 對裝載 SMI-S 服務的伺服器執行探索，則 HP SIM 會找到 ABM 所管理的 EVA4400 陣列。

12.4.1 WEBES 和 EVA4400

針對 ABM 所發行的 CommandView 9.1 版包含 ABM 上執行的 ELMC (WCCProxy)。這可讓 WEBES 取得陣列事件資料的連線點。

WEBES 在 Insight Remote Support Advanced CMS 上執行時，會從 HP SIM 取得受管理實體資訊。請記住，HP SIM 會使用 SMI-S 提供者並透過 WBEM 通訊協定來與陣列進行通訊，而 WEBES 會使用 ELMC (WCCProxy) 的網路連線來與陣列進行通訊。

完成這些步驟以設定 HP SIM 和 WEBES 來監視 EVA4400：

1. 首先，在 WEBES UI 中設定 CommandView 通訊協定認證。這樣可以確保當 WEBES 探索陣列和 ABM 時，會選取正確的 ELMC 通訊協定。
2. EVA4400 ABM 韌體不含 SNMP 或 WBEM 代理程式，所以不支援透過 HP SIM 通訊來擷取硬體資訊。這需要手動設定某些欄位。HP SIM 系統和權限資訊與 WEBES 受管理實體資訊密切相關。WEBES 會偵測 HP SIM 是否存在，並針對新加入的系統或對現有系統所做的變更，將 HP SIM 中已定義的資料填入受管理實體資訊。
3. 已發現在同步化此資訊時，如果遺漏任何必要的欄位，則會造成 WEBES 所探索的實體陷入不完整或無法復原的狀態。這樣可能需要從 WEBES UI 中刪除受管理實體，等到在 HP SIM 中輸入所有必要的資訊後，也必須重新探索受管理實體。停止並重新啓動 DESTA_Service，即可重新探索。

12.4.2 在 HP SIM 中設定 EVA4400 和 ABM

1. 對執行 SMI-S 且已設定爲使用 discoverer.bat 來連線至 ABM 的伺服器執行探索，或對執行 CommandView 並管理陣列的 SMS 執行探索，以開始在 HP SIM 中探索 EVA4400 陣列。
2. 在 HP SIM 中編輯已找到的 EVA 陣列系統內容。包括 Contract and Warranty information、Site Name 及 Primary Contact。您必須填寫這些欄位，HP SIM 才能向 WEBES 受管理實體顯示此權限資料。EVA4400 陣列不需要 Customer-Entered Serial Number 和 Customer-Entered Model Number，因爲 WEBES 會從 EVA 受管理實體的陣列中擷取此資訊。
3. 在 HP SIM 中，探索 ABM，並將 System Name 設爲 ABM 的完整網域名稱。需要此資訊，WEBES 受管理實體才能正確偵測 ABM 並將 ABM 新增爲 EVA 的連線。
4. 在 HP SIM 中編輯已找到的 ABM 系統內容。這是 HP SIM System List 中的保留位置，但還需要其他欄位，WEBES 才能建立受管理實體和通過遠端支援適用性 (RSE) 清單檢查。填寫下列欄位：
   - System type = Storage Device

   
   附註： 需要這些欄位，WEBES 才能正確設定 ABM 實體。

   - System subtype = Storage
   - Product Model = EVA ABM

     需要文字 EVA 才能通過 RSE 檢查。此範例中包含 ABM，以區別 HP SIM UI 中的 ABM 與陣列。

   在 CommandView 使用者介面中選取 **array-name - Hardware- Controller Enclosure**，即可找到此資訊。

12.5 疑難排解 EVA 受管理系統

下列各節特別說明支援 EVA 受管理系統的疑難排解狀況。

12.5.1 HP SIM 未探索 EVA

完成下列區段：

- 「確認 EVA 由目標伺服器上的 CommandView 所管理」
- 「疑難排解 SMI-S 認證」
- 「疑難排解 HP SIM」

12.5.1.1 確認 EVA 由目標伺服器上的 CommandView 所管理

1. 開啓瀏覽器並連線至 CommandView EVA。
2. 選取 EVA 陣列並確認您可以導覽至陣列的元件。
3. 確認 WBEM 通訊協定設定已正確設爲連接埠 5989，且 SMI-S 的使用者名稱和密碼也依照管理陣列的 CommandView 版本正確設定。
   - V8 之前的 cimuser 預設值爲 administrator/administrator
   - V8 之後使用 CommandView 認證
4. 確認 SMS 上正在執行 SMI-S 服務。
   - V8 之前的 HP StorageWorks SMI-S CIMServer。
   - V8 之後的 HP StorageWorks CIM Object Manager
5. 使用 wbemdisco.exe 來測試從 CMS 至 SMI-S 的通訊。如需詳細資訊，請參閱「疑難排解 WBEMDISCO」。

12.5.1.2 疑難排解 SMI-S 認證

SMI-S 必須隨著 CommandView EVA 一起安裝在 SMS 上，才能讓 HP SIM 與 EVA 陣列之間進行 WBEM 通訊協定通訊。CommandView EVA 套件預設會安裝 SMI-S。CommandView V8 中隨附的 SMI-S 提供者與 V6 及 V7 之前版本所提供的 SMI-S 提供者之間，有明顯的改變。

SMI-S 使用 CIMOM 提供者將 WBEM 通訊傳送至 EVA 陣列。從 CommandView V8 開始，SMI-S 使用憑證信任來存取陣列。這與用於 CommandView 登入的使用者名稱和密碼相同。在 CommandView V6 和 V7 中，SMI-S 安裝時採用的使用者認證為使用者名稱=`administrator` 和密碼=`administrator`。在 CommandView EVA 安裝期間，如果採取自訂途徑，則可以變更密碼，將會出現視窗來提示輸入密碼。在 HP SIM System Protocol Settings WBEM Settings 中必須輸入此使用者名稱和密碼。此通訊路徑會使用預設連接埠 5989。

HP SIM 使用這組認證來存取 SMI-S 的 CIMOM 介面。下列程序僅適用於 CommandView V6 或 V7 版本，不適用於 8.0.1 版或更高版本。如果您對使用此密碼有問題而需要重設，或不確定 SMI-S 的使用者名稱和密碼，或者想要新增使用者名稱和密碼，CommandView V6 和 V7 套件隨附一個稱為 `cimuser.exe` 的公用程式，可讓您列出已知的使用者帳戶，在必要時也可以新增或刪除。

若要使用 `cimuser.exe`：

1. 在 SMS 上開啓指令視窗。切換至下列目錄：

   `C:\Program Files\Hewlett-Packard\pegasus_home\bin`

2. 輸入下列指令：

   `cimuser –l (that is, a lower case L)`

   這樣會列出已知的使用者。通常只會列出 `administrator`。

3. 使用下列指令來刪除和重新新增系統管理員帳戶：

   - `cimuser –d –u administrator`
   - `cimuser –a –u administrator`

     系統將會要求您輸入並確認密碼。

12.5.2 疑難排解 HP SIM

1. 設定 WEBES 受管理實體 (平均完成時間視 HP SIM 傳送至 WEBES 的資料而定。可能從幾分鐘至數小時不等)。
2. 在 WEBES SEA Web 介面中，確定 Managed Entities 清單中顯示所有 EVA 裝置。
3. 在 WEBES SEA Web 介面中，確定 Managed Entities 清單中顯示所有 CommandView 伺服器。如果沒有顯示，則表示 HP SIM 中未正確地探索或設定資訊，或該資訊未正確地從 HP SIM 傳送至 WEBES。
4. 刪除 WEBES 擁有的任何 EVA 或 CommandView 伺服器受管理實體、刪除 HP SIM 中找到的 SMS 系統，然後在 HP SIM 中從頭開始探索和設定 SMS 資訊。在 HP SIM 重新找到 SMS 系統後，或後來又修改，該資訊會傳送至 WEBES。
5. 開始測試。

12.5.3 疑難排解 WBEMDISCO

`wbemdisco.exe` 工具是一個 WBEM 探索公用程式，可用來確認對 SMI-S CIMOM 元件的通訊。此程式位於 CMS 上，需要從指令視窗中執行。

1. 在 CMS 上開啓指令視窗，將目錄切換至 `C:\Program Files\HP\Systems Insight Manager`，然後執行 `wbemdisco`。

圖 12-11 執行 wbemdisco

```
C:\Program Files\HP\Systems Insight Manager>wbemdisco

C:\Program Files\HP\Systems Insight Manager>echo Thu 01/10/2008 15:23:28.60
Thu 01/10/2008 15:23:28.60

C:\Program Files\HP\Systems Insight Manager>echo off
WbemDisco 01.00.01
------------------
Gui: Gui starting
Gui: Creating frame...
```

2. 這時會啓動另一個視窗，請輸入SMS節點的名稱。此設定檔名稱和設定會保留供未來使用。圖 4-2

圖 12-12 SMI-S 測試工具

3. 輸入 SMS 節點的 IP 位址 (連接埠 5989 是 SMI-S 的預設連接埠)。
4. 由於 Interop Namespace 指定使用 root/PG_InterOP 做爲認證系統管理員，所以預設密碼應該爲 administrator。如果您已使用 cimuser 來建立不同的使用者名稱/密碼，請改用那些值。

   此步驟在 CommandView V8 中不一樣，Interop Namespace 指定爲 interop，而使用者名稱和密碼認證與 CommandView 登入相同。

圖 12-13 SMI-S 測試工具 (CV 8)

圖 12-14「wbemdisco 輸出」顯示已執行 wbemdisco 指令的指令視窗中的成功輸出：

圖 12-14 wbemdisco 輸出

```
WbemDisco 01.00.01
------------------
Gui: Gui starting
Gui: Creating frame...
HOST    = [illegible]
PORT    = 5989
NAMESP  = root/PG_InterOp
USER    = hpadmins
PASSWD  = ******
Connect to [illegible] in namespace root/PG_InterOp with SSL=true

ObjectManager.Name=PG:AF2BC6C2-2FDC-47F3-BAC7-6935A04D66AA
  ElementName=Pegasus
  CimomVersion=<missing>
  Description=Pegasus CIM Server Version 2.5.1.41 Development

Enumerating instances of CIM_RegisteredProfile...

Profile.RegisteredName=Server
  RegisteredVersion=1.1.0
  ProviderVersion=<no value>
Profile.RegisteredName=Array
  RegisteredVersion=1.1.0
  ProviderVersion=7.0.1
  HPVersion=EVA7.0.1-Dev7
    SubProfile.RegisteredName=Software
    SubProfile.RegisteredName=Pool Manipulation Capabilities and Settings
    SubProfile.RegisteredName=Backend Ports
    SubProfile.RegisteredName=Masking and Mapping
    SubProfile.RegisteredName=LUN Creation
    SubProfile.RegisteredName=Copy Services
    SubProfile.RegisteredName=Block Services
    SubProfile.RegisteredName=Disk Drive Lite
    SubProfile.RegisteredName=FC Target Ports
    SubProfile.RegisteredName=FC Initiator Ports
    SubProfile.RegisteredName=Job control
    SubProfile.RegisteredName=Access Points
    SubProfile.RegisteredName=Location
    SubProfile.RegisteredName=Physical Package Package
    SubProfile.RegisteredName=Multiple Computer System
    SubProfile.RegisteredName=Block Server Performance
  HPEVA_StorageSystem.CreationClassName="HPEVA_StorageSystem",Name="500508B401029910"
    NameSpace  = root/EVA
    Vendor=HP
    Name=EVA
    IdentifyingNumber=500508B401029910
  HPEVA_StorageSystem.CreationClassName="HPEVA_StorageSystem",Name="500508B401024000"
    NameSpace  = root/EVA
    Vendor=HP
    Name=EVA
    IdentifyingNumber=500508B401024000
  HPEVA_StorageSystem.CreationClassName="HPEVA_StorageSystem",Name="50051FE111111000"
    NameSpace  = root/EVA
** CAN'T FIND PhysicalPackage
**   No product information found.

C:\Program Files\HP\Systems Insight Manager>_
```

靠近此輸出上方的 V6 和 V7 失敗表示 cimuser 使用者名稱/密碼驗證有問題，且不會顯示此輸出的大部分內容。請參閱「疑難排解 SMI-S 認證」，其中說明 cimuser.exe 的用法。

傳回的錯誤範例如下：

```
*** Error connecting with SSL=true - (CIM_ERR_ACCESS_DENIED) ***
```

此輸出中間部分所顯示的失敗或錯誤類似 Java 相關的記憶體設定錯誤。請參閱「JAVA 記憶體錯誤」一節。

此畫面結尾的失敗 (未指出 EVA 陣列 WWN 存在) 可能表示：

- EVA 陣列目前不是由此 CommandView 執行個體所管理
- SMI-S 安裝有問題，可能需要解除安裝/清理並重新安裝 CommandView。

SMI-S 記錄檔可能會顯示一些失敗指示，您可以在下列檔案中檢視這些指示：C:\Program Files\Hewlett-Packard\pegasus_home\logs

12.5.3.1 解決通訊失敗的步驟：

1. 停止並重新啓動 SMI-S 服務 HP StorageWorks SMI-S CIMServer 或 HP StorageWorks CIM Object Manager，請參閱「停止 CIMServer」一節。
2. 停止並重新啓動 CommandView 服務 HP CommandView EVA。

3. 解除安裝並重新安裝 CommandView 套件 (包括 SMI-S)。CommandView 和 SMI-S 在解除安裝之後無法完全移除，這是目前已知的問題。可能需要清理登錄項目及檔案和資料夾路徑 (目前正在審核一份定義這些步驟的文件)。
4. 確認 WMI Mapper 連接埠指派。

12.5.3.1.1 停止 CIMServer



附註： 此內容節錄自《CommandView 7.0 版注意事項》：

停止CIMServer服務之後，服務的狀態在服務視窗中會顯示為停止中，但服務不會停止。根據您執行的 Windows 作業系統而定，停用並啓動 CIMServer 服務：

- Windows 2003:若要停止 CIMServer 服務，請移至 [工作管理員]，用滑鼠右鍵按一下 cimserver.exe 處理程序並選取 [結束處理程序]。若要重新啓動 CIMServer 服務，請開啓 [服務] 視窗，用滑鼠按一下 CIMServer，選取 [所有工作]，然後選取 [啓動]。
- Windows 2000:若要停止 CIMServer 服務，請重新啓動系統。若要重新啓動 CIMServer 服務，請開啓 [服務] 視窗，用滑鼠右鍵按一下 CIMServer，選取 [所有工作]，然後選取 [啓動]。這是眾所周知的 Windows 操作。如需詳細資訊，請參閱：http://support.microsoft.com/kb/839174/。若要避免此問題，請不要在啓動 CIMServer 服務之後又立即停止。

12.5.3.1.2 Java 記憶體錯誤：SMI-S EVA 使用者的後置安裝步驟

此資訊收錄在 CommandView 7.0.1 版和 7.0.1 版《版本注意事項》中。

根據預設，JVMOptions.conf 檔案中的 -Xmx 值會設為 1024m，但這不一定永遠都是正確的值。若要決定 -Xmx 的正確值，請在安裝 HP StorageWorks CommandView EVA 軟體套件 7.0.1 之後立即完成下列步驟：

1. 在指令行中，輸入安裝目錄:\Program Files\Hewlett-Packard\pegasus_home\jre\bin\java" -Xmx1024m –version。如果傳回 Java 版本號碼，則表示 -Xmx 的預設值 1024m 是正確的。如果未傳回 Java 版本號碼，請以較小的值重試指令，直到某個值傳回 Java 版本為止。
2. 在位於 OS 安裝目錄:\Program Files\Hewlett-Packard\pegasus_home 目錄的 JVMOptions.conf 檔案中，將傳回 Java 版本的值新增為 -Xmx 值。



重要： Java 相關建議：

注意：使用舊版的Java Runtime Environment (JRE) 時，HP StorageWorks CommandView EVA 6.X 版安裝和升級不正常：

此建議的重要聲明：安裝機制要求在管理伺服器上安裝最新版的 JRE。您可以從下列 URL 下載 JRE：http://java.sun.com/javase/downloads/index.jsp

12.5.3.1.3 SMA 上的 CommandView SSO 憑證：將 SSO 憑證新增至 CommandView EVA truststore 信任庫

《CommandView 7.0 版版本注意事項》中說明此資訊：

1. 若要在儲存管理設備中將 SSO 憑證新增至 CommandView EVA truststore信任庫，請在安裝 HP StorageWorks CommandView EVA 軟體套件 7.0 之後完成下列步驟：導覽至 \Program Files\Hewlett-Packard\pegasus_home\bin\EVAProvider 目錄。執行 genEVACert.bat 檔案；將會更新 truststore 信任庫。
2. 若要確認已安裝 truststore 信任庫，請完成下列步驟：在 CommandView EVA GUI 中，按一下 Server Options。按一下 Other application trust relationships。您可以檢視已安裝的憑證。

12.5.4 疑難排解 SMS 上的 ELMC 安裝

問題：

SMS 上的 ELMC 安裝失敗。此問題可能起因於 Windows Management Instrumentation (WMI) 服務阻止存取所需的系統檔案。

解決方案

解決方案是使用 Windows Services Manager 公用程式停止 WMI 服務，將檔案解除鎖定，安裝 ELMC，然後重新啓動 WMI 服務。

12.5.5 使用 RSCC 來收集 EVA 資料之前停用 HPCC

如果您想要使用 Remote Support Configuration Collector (RSCC) 來執行 EVA 資料收集，您必須確定儲存管理伺服器 (SMS) 上沒有執行 HP ISEE Configuration Collector (HPCC) 元件。若要停用 HPCC 元件，請執行下列步驟：

1. 在 HP ISEE Configuration Collection for EVA 主機 (SMS) 上，選取**開始>控制台>系統管理工具>服務**，以顯示服務清單。
2. 找到 EVA 服務的 HP ISEE Configuration Collector。以滑鼠右鍵按一下並選取 [內容]。
3. 從 [啓動類型] 下拉式功能表中選取 **[已停用]**。
4. 按一下 **[停止]**，按一下 **[確定]**，再按一下 **[關閉]**。

13 適用於 Insight Remote Support Advanced 支援之 San Switch 與磁帶櫃的需求

13.1 系統需求

- 在 CMS 上，WEBES 5.6 + Update 1 對於 FC Switch 和 Nearline 磁帶櫃支援而言是必要的，且支援虛擬和實體的資料備份櫃。CMS 上的 RSSWM 應用程式將可讓您下載並安裝 WEBES 5.6 + Update 1 (請遵循《 `Insight Remote Support Advanced CMS with WEBES 5.6 Configuration and Usage Guide.`》中的指示)。因爲您必須在完成 San Switch 或資料備份櫃設定之前，先在 CMS 上安裝 WEBES，所以需要在完整設定 CMS 之後重新造訪本節。
- 所有的受管理系統都必須設定，才能將 SNMP v1 trap 傳送至 CMS。
- 您可能也需要設定交換器，以允許 CMS 和交換器之間的 SNMP 通訊。
- DCFM 必須位於適合將 McData FC 交換器事件轉送至 CMS 的環境中。

13.2 受管理系統設定

CMS 上的 HP SIM 必須能夠找到及辨識每個 FC 交換器或虛擬和實體資料備份櫃系統。

13.2.1 設定詳細資訊

請注意：

- 確認 HP SIM 已辨識出客戶環境中的每個 FC 交換器。別忘記設定交換器應用程式，以便將 trap 傳送至 CMS。
- 確認 HP SIM 已擷取交換器的正確產品編號及序號資訊。
- 修改 HP SIM 中任何不正確或遺失的合約識別碼及客戶連絡人詳細資訊。
- 確認已針對受管理裝置 (受管理系統) 選取最適當的系統類型。



附註： 除非 HP SIM 已辨識出交換器，否則將無法提升事件。

13.3 San Switch 設定

13.3.1 Brocade SNMP 設定

請執行下列步驟 (這其中包含大部分的 HP StorageWorks 光纖通道交換器)，來設定 Brocade SNMP：

1. 透過 Telnet 登入 CLI 介面，或者使用 Brocade Switch Explorer 來登入。
2. 使用 CLI 指令 `agtcfgset` 或更新的 `snmpconfig`，以進入 SNMP 設定模式。
3. 如果您選取非標準的 trap 社群名稱 (例如，`public` 以外的名稱)，請確定 CMS 上的 HP SIM 可以辨識此名稱。
4. 將 CMS 的 IP 位址輸入其中一個 trap 目的地設定。
5. 設定 **mibCapability** 以啓用 `SW-TRAP`、`FA-TRAP` 和/或 `HA-TRAP` MIB trap (您必須針對此工作使用 CLI)。
6. 如果存取控制清單含有任何項目，請確定 CMS 的網域也包含在此清單中。此設定也可以透過內嵌交換器的 Web 介面來完成。請參閱交換器設定手冊，以取得如何設定 trap 嚴重性層級和 MIB 功能的詳細資訊 (如有需要)。
7. 在 Managed Systems 頁面中輸入詳細資訊，並針對品牌爲 Brocade 之交換器的系統類型選取 **B series FC switch**，或者針對 HP StorageWorks FC 交換器選取 **FC switch**。此程序記錄於《`HP Insight Remote Support Advanced CMS 設定與使用手冊`》的第五章中。

13.3.2 Cisco FC 交換器 SNMP 設定

請執行下列步驟來設定 Cisco SNMP：

1. 透過 Telnet 登入 CLI 介面，或者使用 Fabric Manager 來登入。
2. 使用 CLI 指令 `config t` 和 `snmp-server host <IP> traps version 1 public udp-port 162` 指令，將 CMS IP 位址新增爲 trap 目的地。
3. 選擇以取得傳回爲 trap 的所有事件。
4. 如果您選擇非標準的 trap 社群名稱 (例如，`public` 以外的名稱)，請確定 CMS 內部設定頁面上包含此名稱。
5. 將 CMS 的 IP 位址輸入其中一個 trap 目的地設定。此設定也可以透過 Cisco Device Manager 來完成。
6. 在 CMS 的 Managed Systems 頁面中輸入詳細資訊，並針對品牌爲 Cisco 之交換器的系統類型選取 **C-series FC switch**。

13.3.3 設定 McDATA 光纖通道交換器 (M/系列)

DCFM 10.3.0 伺服器是已安裝 DCFM 應用程式的 PC 設備。此應用程式先前稱爲 HAFM 或 EFCM。唯有 DCFM 10.3.0 版或更高版本能夠將事件傳送至 CMS。此應用程式提供操作和管理 M/系列 FC 交換器的介面，並且可將交換器事件資料透過 HTTP 轉送至 CMS。請遵循下列步驟來設定 DCFM，並將 DCFM 伺服器連接至 CMS。

1. 在 DCFM **Discover** →**Setup** 功能表內找到 McData 交換器。
2. 存取 Call home 設定功能表 **Monitor** → **Event Notification** → **Call home**。
3. 在產品清單下方選取 McData 交換器，然後將他們新增至 Call Home 窗格的 HP LAN 區段中。
4. 按一下 **Edit Center**，然後將 CMS 的 IP 位址新增爲 **Service Gateway**。
5. 套用設定，若您想要測試連線，可以按一下 **Send Test** 按鈕。
6. 按一下 **Call Home** 對話方塊中的 **Apply**，或者按一下 **OK**。

   不需要套用任何 Call Home 篩選。
7. 最後，請移至每個受管理的 M/系列裝置，並啓用 **phone home**。

13.3.3.1 HP QLogic 交換器設定

透過 Telnet 登入交換器，並發出下列 CLI 指令來設定 HP 8/20q 或 2/8q FC 交換器，以便將 SNMP trap傳送至 CMS。

```
Admin begin
Set setup SNMP (configure the trap destinations)
"y" to save and activate the configuration
Admin end
```

13.3.3.2 HP VC-FC 虛擬連接模組設定

請執行下列步驟來設定 HP VC-FC 虛擬連接模組：

1. 登入 On-Board Administrator，然後在左窗格中選取 Virtual Connect manager。
2. 一旦位於 VC manager 中，請選擇左側的 SNMP 設定選項。
3. 在 **SNMP alert destination** 區段中，輸入 CMS 的 IP 位址和社群名稱。請注意，您只能在 VC manager 中輸入一個目的地 IP 位址。相同的目的地將套用至所選取 OA 之控制項下方的所有 VC-FC 模組。
4. 在 CMS 受管理系統頁面中輸入詳細資訊，並針對 HP StorageWorks 虛擬連接 FC 交換器模組的系統類型選取 **FC switch**。

13.3.4 VLS/ETLA/MCS MSL G-3 SNMP 設定

13.3.4.1 CV-TL 和 CV-VLS SNMP 設定

1. 登入每個 VLS/ETLA 的 Command View VLS/TL Web 介面。
2. 按一下 **Notifications** 標籤。
3. 按一下 **Edit SNMP settings** 工作。
4. 在 **Hostname** 欄位中，輸入 CMS IP 位址或名稱。
5. 除非您已定義其他社群字串，否則請輸入 **public** 做爲社群字串。
6. trap 版本是 `1`。
7. 按一下 **Add**。

13.3.4.2 CV-MSL SNMP 設定

1. 以 **Administrator** 身分登入 Command View MSL Web 介面。
2. 按一下 **Configurations** 標籤。
3. 按一下 **Network Management** 標籤。
4. 確認已選取 **SNMP**。
5. 在 **IPv4 target address** 欄位中輸入 CMS 的 IP 位址。
6. 確認已選取版本 `SNMPv1`。
7. 選取 **Critical and Warnings** 做爲篩選層級。
8. 按一下 **Submit**。

13.3.5 測試設定



附註： 請勿提取備援的 FRU，來測試支援之交換器或資料備份櫃的設定。

13.3.5.1 測試 Cisco 交換器設定

Cisco 最近引進了一個 CLI 測試指令，可用以驗證裝置的端對端事件連線。

1. 從 CLI 提示中，發出下列指令：

```
test pfm test-SNMP-trap power
```

2. 這樣會導致Cisco交換器將僞裝損壞的電源供應器事件傳送至CMS。如果所有項目均已正確設定，則此事件將會產生可在 HP 上檢視的事件。



附註： 您也可以使用 `test pfm test-SNMP-trap fan`，但是將會忽略 `temp` 類型事件 (如果已使用)。

13.3.5.2 測試 VLS 設定

使用最新的 VLS 韌體及最新版的 Command View VLS，找到 CV-VLS SNMP 設定頁面上的 **Test SNMP** 按鈕以執行端對端測試。此測試事件將不會在 HP 方建立任何結果，但是它將會建立一個本機電子郵件通知，以做爲 VLS SNMP 和 CMS 已正確設定的確認。

13.4 Nearline(磁帶櫃) 設定

磁帶櫃 RSS 和 RSA 設定會使用 HP Command View 管理工具

13.4.1 CV-TL SNMP 設定

1. 登入每個 ESL 或 EML 的 Command View TL Web 介面。
2. 按一下 **Configuration** 標籤。
3. 在左面板中，選取 **SNMP Alerts**。目前的 SNMP trap便會顯示於右面板中。

4. 執行下列其中一個動作：
   - 在右面板中，用滑鼠右鍵按一下 SNMP trap，然後選取 **Add Trap Entry**。

     或者

   - 選取 **Actions** → **Add Trap Entry**。
5. 隨即會出現 **SNMP Trap Entry** 對話方塊。
6. 在 **Trap Destination** 欄位中，輸入 WEBES 主機 IP 位址或名稱。
7. 除非您已定義其他社群字串，否則請輸入 `public` 做爲 **Community String**。
8. 最後按一下 **OK**。

13.4.2 CV-VLS SNMP 設定

1. 登入每個 VLS 節點的 Command View VLS Web 介面。
2. 按一下 **Notifications** 標籤。
3. 按一下 **Edit SNMP settings** 工作。
4. 在 **Hostname** 欄位中，輸入 WEBES 主機 IP 位址或名稱。
5. 如果您選取非標準的 trap 社群名稱 (例如，`public` 以外的名稱)，請確定 CMS 上的 HP SIM 可以辨識此名稱。
6. trap 版本是 `1`。
7. 最後按一下 **Add**。

13.4.3 CV-MSL (MSL G3) SNMP 設定

1. 以 `Administrator` 身分登入 Command View MSL Web 介面。
2. 按一下 **Configuration** 標籤。
3. 按一下 **Network Management** 標籤。
4. 確定已勾選 **SNMP**。
5. 在 **Ipv4 target** 位址欄位中輸入 WEBES 主機的 IP 位址。
6. 請確定已選取版本 **SNMPv1**。
7. 選取 **Critical and Warning** 做爲篩選層級。
8. 按一下 **Submit**。

13.4.4 測試設定

我們不建議您提取備援的 FRU 來測試設定。如果您擁有最新的 VLS 韌體及最新版的 Command View VLS，則 CV-VLS SNMP 設定頁面上會有一個 **Test SNMP** 按鈕可執行端對端測試。此測試事件將不會在HP方建立任何結果，但是它將會建立一個本機電子郵件通知，以做爲VLS SNMP 和 WEBES 已正確設定的確認。

14 使用目標型 SNMP 支援來設定 MSA 受管理系統

您必須確認下列事項後，才能監視 Modular Smart Array (MSA)：

- 查看《`A.05.40 Insight Remote Support Advanced Release Notes`》，確認該系統是支援的系統。
- 確認您的受管理系統上已適當設定 SNMP。

14.1 關於 MSA 目標型 SNMP 支援

下列幾種 Modular Smart Array (MSA) 使用目標型 SNMP 支援進行 Insight Remote Support Advanced 監視。

- 1510i
- 2012 和 2112
- 23xx

每種受管理系統類型的 MSA 出廠時應該都已在裝置上安裝 SNMP。若要使用目標型支援，您必須在支援的 Web 瀏覽器中使用個別的介面來設定 SNMP，以支援上述系統類型。

14.2 關於 MSA 目標型 SNMP 支援

下列幾種 Modular Smart Array (MSA) 使用目標型 SNMP 支援進行 Insight Remote Support Advanced 監視。

- 1510i
- 2012 和 2112
- 23xx

每種受管理系統類型的 MSA 出廠時應該都已在裝置上安裝 SNMP。若要使用目標型支援，您必須在支援的 Web 瀏覽器中使用個別的介面來設定 SNMP，以支援上述系統類型。

14.2.1 MSA 1510i

完成下列步驟來存取 MSA 1510i，並設定 Insight Remote Support Advanced 支援的 SNMP：

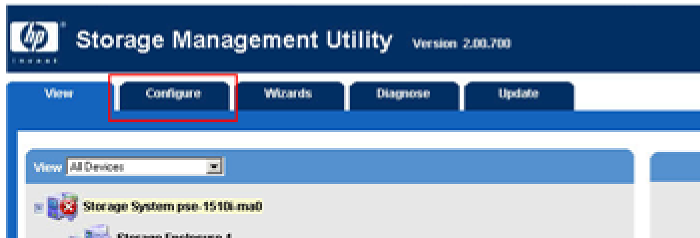
1. 登入 HP StorageWorks MSA Storage Management Utility





附註： 如需設定此工具和管理認證的基本資訊，請參閱 StorageWorks 文件。

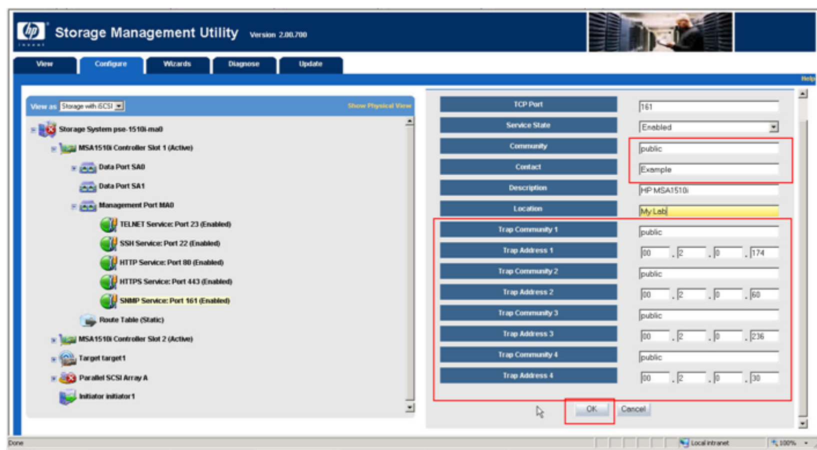
2. 登入此公用程式之後，選取 **Configure** 標籤。



3. 在 **Configure** 標籤上，展開 MSA 1510i 的 **Management Port** 清單。
4. 從清單中選取 **SNMP Service** 連結。



5. 修改任何必要的設定欄位，並確定 CMS 的 IP 位址已列爲 **Trap Address**。
6. 按一下 **OK**，認可您所做的變更。

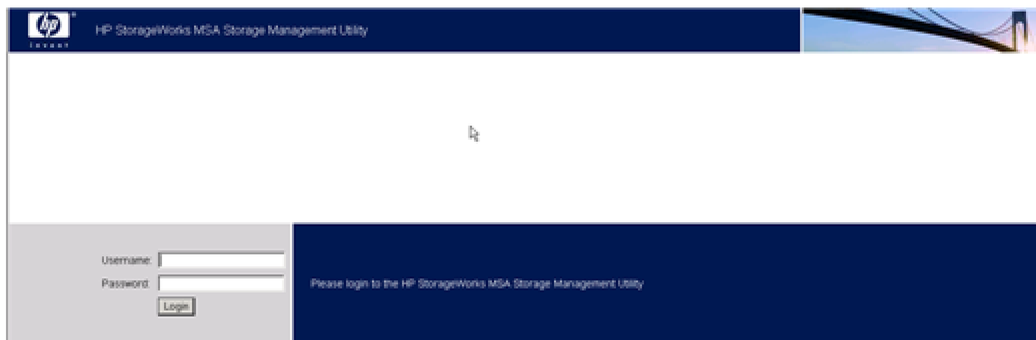


7. 結束公用程式，確認 CMS 上的 HP SIM 已找到您的 1510i。

14.2.2 MSA 2012 或 2112 系列

完成下列步驟來存取 MSA 2012 或 2112，並設定 Insight Remote Support Advanced 支援的 SNMP：

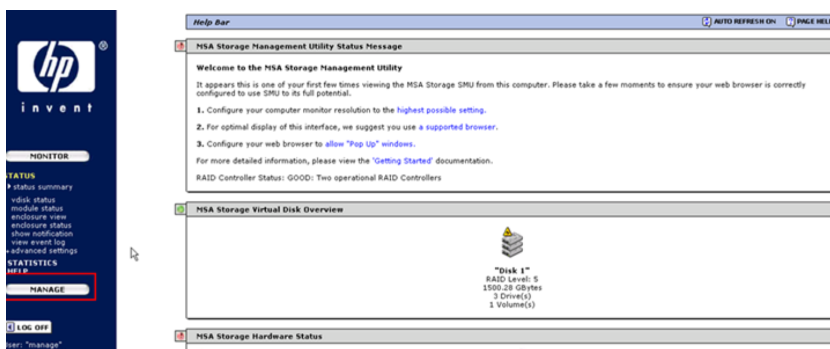
1. 登入 HP StorageWorks MSA Storage Management Utility



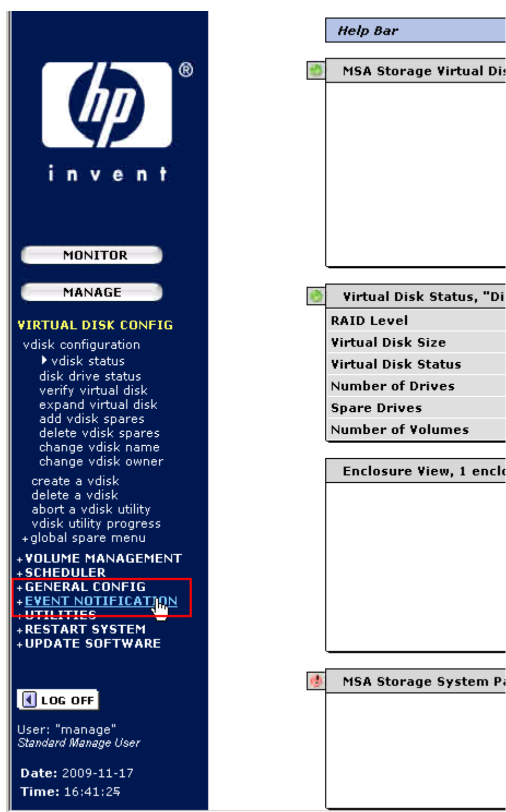


附註：　如需設定此工具和管理認證的基本資訊，請參閱 StorageWorks 文件。

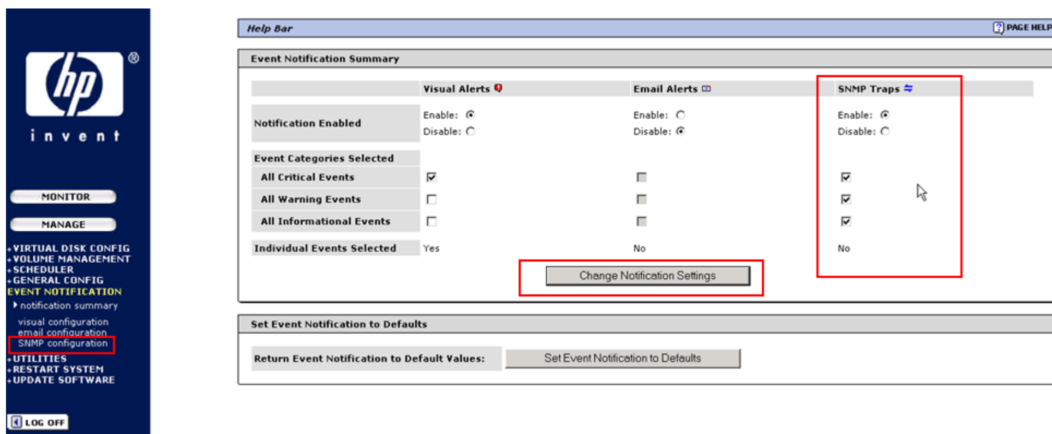
2. 登入此公用程式之後，選取 **Manage** 按鈕。



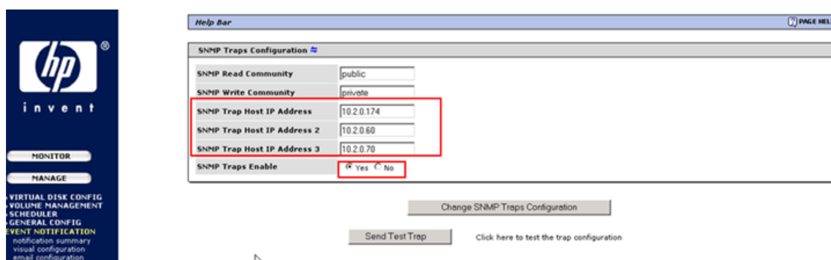
3. 在展開的清單中，選取 **Event Notification** 連結。



4. 在 **Event Notification** 頁面上，確認已啓動 SNMP 通知類型 (建議三種全部選取)，然後按一下 **Change Notification Settings** 認可變更。



5. 在左邊面板的 **Event Notification** 清單下，按一下 **SNMP configuration** 連結。
6. 修改 SNMP 設定將 CMS 納入爲 Test Trap Host，並確定 **SNMP Test Traps Enabled** 圓鈕已設爲 **Yes**。



7. 按一下 **Change SNMP Test Traps Configuration**，認可您所做的變更。



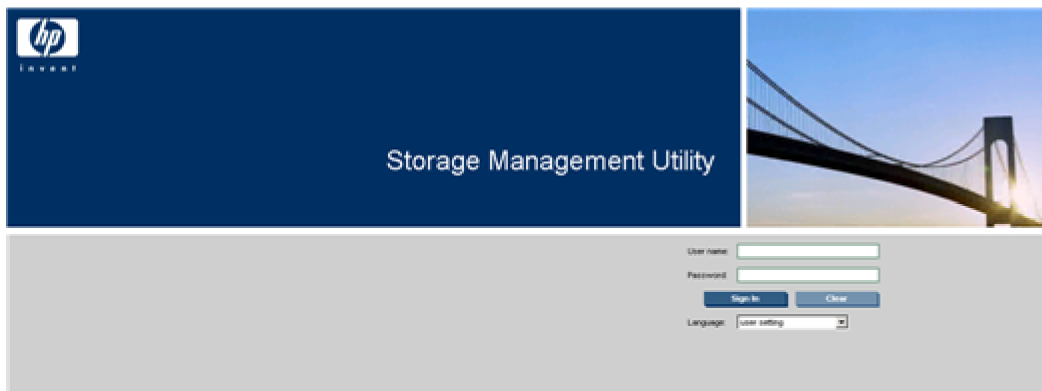
附註： 如果 Insight Remote Support Advanced CMS 已完整設定，您可以從這個頁面傳送測試事件。如果 CMS 尚未設定，您稍後可以回到這個頁面來傳送測試事件。

8. 結束公用程式，確認 CMS 上的 HP SIM 已找到您的 2012/2112。

14.2.3 MSA 23xx 系列

完成下列步驟來存取 MSA 23xx，並設定 Insight Remote Support Advanced 支援的 SNMP：

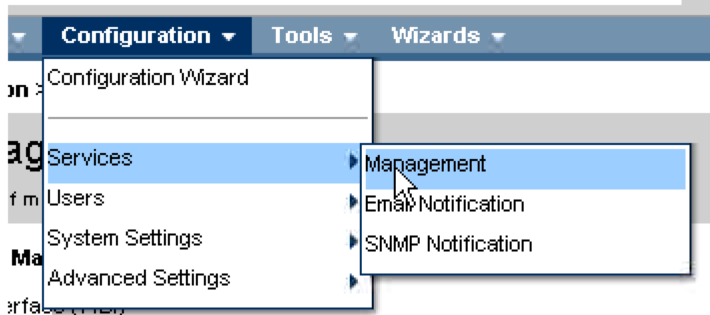
1. 登入 Storage Management Utility





附註： 如需設定此工具和管理認證的基本資訊，請參閱 StorageWorks 文件。

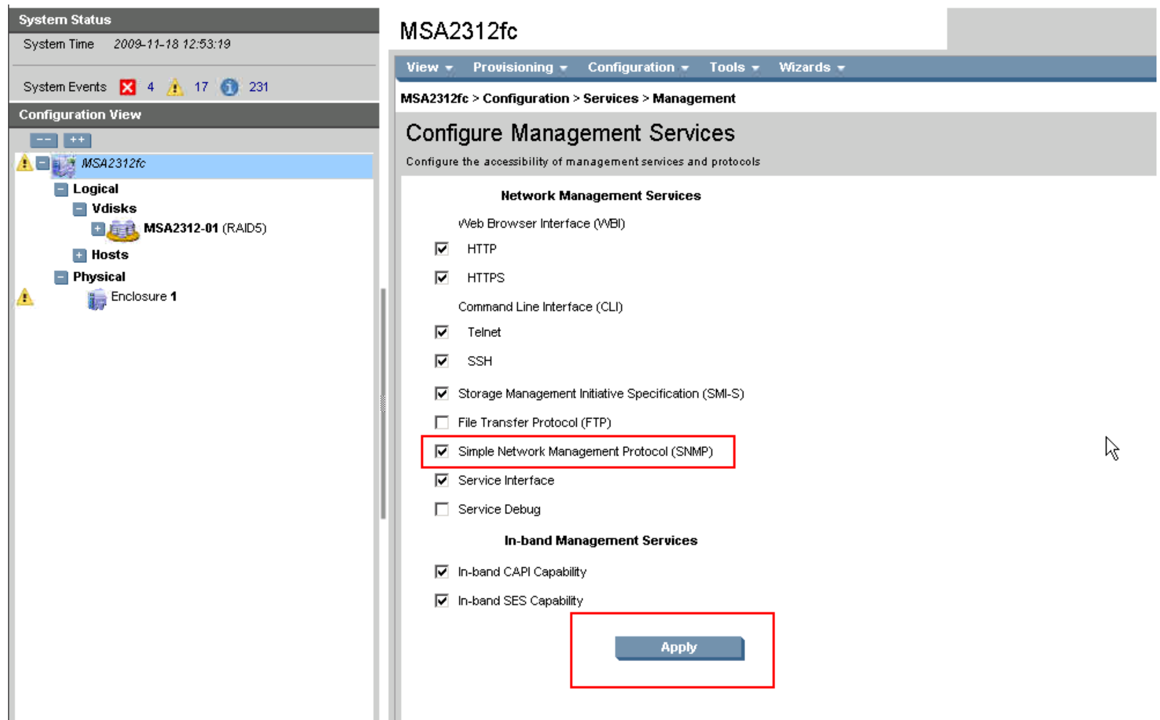
2. 登入此公用程式之後，選取 **Configuration > Services > Management**。



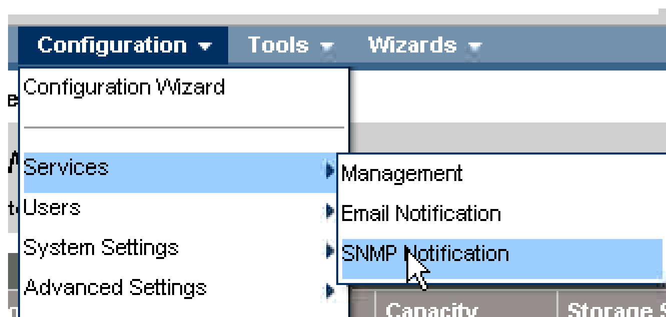
3. 確定從 **Network Management Services** 清單中選取 SNMP，然後按一下 **Apply**。



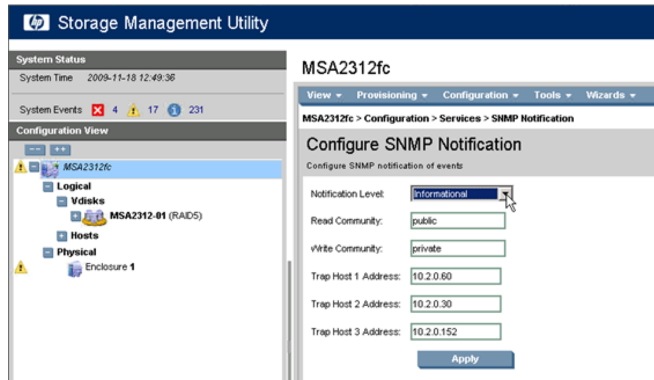
重要： SNMP 預設應該爲作用中，但如果由於任何原因而不在作用中，則不會支援 Insight Remote Support Advanced。必須確認 SNMP 在作用中。



4. 從功能表中，選取 **Configuration** → **Services** → **SNMP Notification**。



5. 在 **Configure SNMP Notification** 頁面上，修改 SNMP 設定將 CMS 納入為 Test Trap Host，然後從下拉式功能表中選取 **Notification Level** (建議選取資訊 (Information) 層級)。



6. 按一下 **Apply**，認可您所做的變更。
7. 結束公用程式，確認 CMS 上的 HP SIM 已找到您的 23xx。

15 設定主機型 MSA

您必須確認下列事項後，才能監視主機型 MSA：

- 查看《`A.05.40 Insight Remote Support Advanced Release Notes`》，確認主機系統是支援的受管理系統。
- 確認主機系統已適當地設定成使用 OpenVMS 或 Tru64 Unix 的受管理系統，且已依照本文中相關章節的指示來設定。

如果 MSA 已根據製造商的指示正確設定，則應該能夠與主機進行通訊。如果主機已依照本文的指示適當地設定成受管理系統，則主機/受管理系統就能夠將您的 MSA 事件資訊傳送至 CMS，以進行遠端支援。

詞彙表

Event Log Monitoring Collector (ELMC)
ELMC (先前稱 WCCProxy) 會提供事件日誌檔的錯誤狀況偵測，並將這些事件傳遞至 WEBES。

HP Care Pack Services
HP Care Pack 可隨同 HP 產品與服務一起購買，以透過增強的支援套件升級或延長標準保固期間。這些支援套件可降低停工的風險，支援層級從基本到關鍵。

許多產品在其原始保固期到期後，也可取得保固後 HP Care Pack Services 服務。

HP System Management Homepage (SMH)
HP System Management Homepage (SMH) 是一種網頁式介面，將 HP-UX、Linux 和 Windows 作業系統上的 HP 伺服器合併並簡化成單一系統管理。

HP Systems Insight Manager (HP SIM)
HP Systems Insight Manager (HP SIM) 是統一伺服器與儲存管理平台。系統管理員可從單一的管理主控台使用安全管理工具組來管理其完整的 HP 伺服器與儲存環境。

Insight Remote Support Advanced
Insight Remote Support Advanced 可主動進行遠端監控、診斷與疑難排解，以協助提升您資料中心內 HP 所支援伺服器與儲存系統的可用性。HP Remote Support 可透過系統的支援來降低成本與複雜性。HP Remote Support 可將硬體事件資訊安全地通過您的防火牆和/或 Web proxy，傳遞至 HP 支援中心以進行反應式支援。此外會根據您支援服務合約的內容，決定是否收集系統資訊進行主動式分析與服務。

OSEM (Open Service Event Manager)
安裝在 CMS 上的 Remote Support 元件，可透過產品特定的規則集執行即時服務事件篩選。這些規則集會定期視是否有可用的改進功能予以更新。

Remote Support Services
Remote Support Services 可讓您啓用或停用您企業中所有合格系統的遠端支援。Remote Support Services 也會顯示合格系統其 Remote Support 授權檢查的狀態，並提供 Remote Support 授權檢查的存取權。

Remote Support 合格系統
執行 Windows 2003 或 Linux Red Hat 的 HP ProLiant 伺服是合格的系統，當啓用時會將事件傳送至 HP 支援中心來解決事件。系統也必須具備 Remote Support 的資格，否則將會關閉傳送的事件。您可以使用 Remote Support Services 中的 Remote Support 授權檢查來確認合格的系統確實受到支援。

Remote Support 授權檢查 (RSEC)
RSEC 是一種檢查功能，會檢查 HP 權益資料存放區中特定系統的目前義務狀態。RSEC 視窗會顯示 Remote Support 授權檢查的結果，透過 **Remote Support Services** 標籤的 `Support Obligation` 欄可存取此視窗。

Remote Support 設置
Remote Support 設置是一個集合點，集合了您公司的企業合約資訊、指定的企業支援聯絡資訊，以及您的 HP 客戶團隊聯絡資訊。

Storage Management Server (SMS)
安裝 HP StorageWorks Enterprise Virtual Array (EVA) 軟體的系統，包括 HP Command View EVA 與 HP Replication Solutions Manager (若有使用)。它是專用的管理系統，專門執行 EVA 管理軟體。

Web Based Enterprise Management (WBEM)
Web Based Enterprise Management (WBEM) 是一組管理與網際網路標準技術，這些技術是爲了統一管理分散式運算環境而開發。

基本上，WBEM 是業界的首創，可標準化不同平台間的管理資訊。

Web-Based Enterprise Service (WEBES)
安裝在 CMS 上的 Remote Support 元件，可透過產品特定的規則集執行即時服務事件分析。這些規則集會定期視是否有可用的改進功能予以更新。

中央管理伺服器 (CMS)
管理網域中執行 HP Systems Insight Manager 軟體的系統。HP Systems Insight Manager 中的所有中央作業皆從此系統開始執行。

企業虛擬陣列 (EVA)
EVA 是高效能、高容量與高可用性的虛擬 RAID 儲存解決方案，適合高階企業環境。

完整設定權限使用者
自動獲得授權可在所有系統上使用 **All Tools** 工具箱 (包括 CMS) 的使用者。這一類型的使用者已獲得可管理 HP Systems Insight Manager 軟體的特殊權限。

系統 網路上的節點，透過 TCP/IP 或 IPX 進行通訊。若要管理系統，系統上必須有某種類型的管理通訊協定 (例如 SNMP、DMI 或 WBEM)。例如伺服器、工作站、桌上型電腦、可攜式裝置、路由器、交換器、集線器和閘道等，都可稱做系統。

系統故障管理 (SysFaultMgmt 或 SFM) SFM 是實作 WBEM 標準的 HP-UX 錯誤管理解決方案。SysFaultMgmt 與其他如 HP SIM、HP SMH 等容易管理的應用程式，和任何其他的 WBEM Client (例如 WEBES) 整合在一起。

使用者 能夠有效登入 CMS 且已新增至 HP Systems Insight Manager 的網路使用者。

探索 管理應用程式的一項功能，可尋找與識別網路物件。在 HP 管理應用程式中，探索會尋找並識別指定網路範圍內所有的 HP 系統。

設定資料集合 HP SIM 使用集合一詞來指稱受管理系統的群組，Insight Remote Support Advanced 則使用設定集合一詞來指稱從受管理系統中收集到的資料。此資料會傳遞至 HP 以進行主動式分析。

集合 使用 HP SIM 時，一種群組系統或事件搜尋的方法。

網域名稱服務 (DNS) 一種將網域名稱轉換成 IP 位址的服務。

網際網路通訊協定 (IP) 指定資料包 (封包) 的格式，以及網路上的定址設定。大多數的網路會將 IP 與傳輸控制通訊協定 (TCP) 結合在一起，在目的地與來源之間建立虛擬連線。

遠端支援軟體管理員 (RSSWM) HP 遠端支援軟體管理員是安裝在 CMS 上的應用程式，並隨附下載與安裝在 CMS 上 SIM 所需的 Insight Remote Support Advanced 元件。

儲存設備區域網路 (SAN) 儲存設備區域網路 (SAN) 是由儲存裝置和啓動器構成的網路，啓動器用於儲存與擷取儲存裝置上的資訊，包括通訊基礎結構。在大型企業中，SAN 會將多個伺服器連接至磁碟儲存區的中央集區。相較起管理數百台有各自磁碟的伺服器，SAN 能改善系統管理作業。

簡易網路管理通訊協定 (SNMP) HP Systems Insight Manager 支援的管理通訊協定之一。網路系統與多數伺服器廣泛使用的傳統管理通訊協定。MIB-2 是標準資訊，可持續供所有的廠商使用。

識別 探索程式的一個層面，可識別管理通訊協定與系統類型。

索引